Multimedia Tools and Applications (2021) 80:4789–4823
https://doi.org/10.1007/s11042-020-09881-8

Efficient HEVC steganography approach based on audio compression and encryption in QFFT domain for secure multimedia communication

Naglaa F. Soliman[1,2] · M. I. Khalil[3] · Abeer D. Algarni[1] · Sahar Ismail[1,4] · Radwa Marzouk[1,5] · Walid El-Shafai[6]

Received: 27 May 2020 / Revised: 17 August 2020 / Accepted: 15 September 2020 /
Published online: 1 October 2020

Abstract
High-Efficiency Video Coding (HEVC) is the most recent video codec standard. It is substantial to analyze the HEVC steganography process due to its practical and academic significance. Thus, a secure HEVC steganography approach is introduced in this paper to study the possibility of hiding an encrypted secret audio message within a cover compressed video frame in a secure and complicated manner. In the preliminary stage, the secret audio message is compressed utilizing the Discrete Cosine Transform (DCT) to achieve a high capacity performance for the HEVC steganography process. After that, the suggested approach implies two-cascaded encryption layers to encrypt the compressed secret message before embedding it within a cover HEVC frame. In the first encryption layer, a novel encryption technique based on random projection and Legendre sequence in the Discrete Wavelet Transform (DWT) domain is introduced to cipher the compressed secret audio message. In the second encryption layer, the yielded encrypted audio message is represented in a form of quaternion numbers using the Quaternion Fast Fourier Transform (QFFT) technique. Each cover HEVC frame is also represented in a quaternion form. In the suggested approach, some straightforward quaternion mathematical operations are employed on the encrypted secret message and the cover HEVC frames to represent them in a quaternion form in the frequency domain, then the encrypted secret audio message is hidden within the cover HEVC frame. At the receiver, the secret message can be retrieved and extracted from the cover HEVC frame utilizing the same methodology of the employed quaternion mathematical operations. The major contributions of the suggested HEVC steganography scheme are: (1) it allows hiding of massive amount of secret information within cover video frames, and (2) it has higher robustness against multimedia attacks and steganalysis contrasted to the conventional and literature schemes. Furthermore, the proposed approach is evaluated utilizing different assessment metrics like Feature Similarity Index Measure (FSIM), Peak Signal-to-Noise Ratio (PSNR), correlation coefficient, and

✉ Walid El-Shafai
walid.elshafai@el–eng.menofia.edu.eg; eng.waled.elshafai@gmail.com

Extended author information available on the last page of the article

Structural Similarity Index Measure (SSIM) to evaluate the efficiency of the stego HEVC frames compared to the original ones. The achieved outcomes demonstrate that the suggested steganography scheme is straightforward to implement, more secure, and robust in the presence of steganalysis multimedia attacks compared to the literature approaches.

Keywords Quaternion mathematics · HEVC steganography · QFFT · Random projection · Legendre sequence · DCT · DWT

1 Introduction

Network security is becoming increasingly important as more and more data is exchanged over the Internet. Therefore, data security and confidentiality are essential today to prevent any unauthorized access, and so there is a great growth of the information hiding field. Information hiding techniques have been performed efficiently on different applications like army and radar applications, healthcare applications, anti-criminal, and commercials [16, 21, 22]. To solve the problem of the protection-hidden message, there are three methods that can be employed which are cryptography, watermarking, and steganography [16].

Cryptography converts a plain message to an unreadable one, called cipher message. To decipher this unreadable message, a secret key is required that is used in an algorithm for performing the encryption process or decryption process [6, 39]. Watermarking and steganography are also used for the purpose of data hiding through hiding media in other media. In the steganography process, hiding the data cannot be seen or detected [3, 25, 28]. However, in the watermarking process, the information may not be completely hidden, as it should be secure, and a watermark is embedded into the data to save the privacy of the user. So, watermarking is the procedure of hiding data into multimedia information without observing from the humans, however, this data is clearly discovered by a detector or a computer. So, the watermarking process is suitable for a lot of applications and services like authentication, fingerprinting, copy control, and copyright protection. The watermarking process involves an embedding process and an extraction process, which has many features like robustness, fidelity, and tamper-resistance [2, 30].

Steganography has become an essential process for identification and authentication applications. Steganography can be applied to several types of data such that audio, video, and images, and it can hide any kind of digital information. Steganography and steganalysis are two contending concepts [43]. Steganalysis art is the science of identifying the hidden data concealed in digital multimedia information utilizing the steganography process, which called steganography detection. It can lead to the avoidance of unfortunate security incidents. The amount of hidden data compared to the size of the cover multimedia data will determine the detection ability. There are various steganalysis methods like carrier comparison, structural inspection, and statistical analysis. Steganalysis is divided into two main categories of analysis: statistical and visual analyses [54].

The main classification of steganography techniques is spatial domain-based schemes, frequency domain-based schemes, and adaptive schemes. The spatial domain-based schemes are generally classified into the Pixel Value Difference (PVD) schemes, the Least Significant Bit (LSB) schemes, and the machine learning-based schemes [13]. In the LSB methods, hidden data is distributed among the LSBs of each pixel. The PVD methods are utilized to differentiate the smooth areas from the edge areas. The machine learning is considered as a

subset of artificial intelligence, which provides the ability to learn without being programmed. Frequency domain-based techniques include the Discrete Cosine Transform (DCT) and DWT. They are used to convert an image or a video frame to a frequency domain from its original form in a spatial domain [23, 47]. These methods are slower and difficult than spatial domain-based methods since a cover image or a cover video frame should be transformed into the frequency domain coefficients before embedding the secret information. Each one of these methods has its own advantages and disadvantages [1].

Both cryptography and steganography can be used to get more confidentiality and privacy of data and keep it secret. The steganography process varies from the cryptography process in that steganography concentrates on maintaining the existence of a data secret, while cryptography concentrates on preserving the contents of a data secret [14, 40]. Many researchers have developed various steganography algorithms to retain confidentiality by embedding the data in various carriers like video, image, audio, and text [10, 41]. Noda et al. [36] developed a steganography technique that is based on the lossy compressed video to embed large data in its frames. The Bit Plane Complexity Segmentation (BPCS) steganography method is utilized in the proposed technique. Also, the wavelet compression is utilized for compressing the video data. Thus, the Motion-JPEG2000 and 3-D Set Partitioning In Hierarchical Trees (SPIHT) wavelet-based video coding approaches are utilized. The wavelet coefficients in the video frames are quantized into an arrangement of bit-planes, and hence the steganography process of the BPCS can be performed in the wavelet domain. Also, the integration of the Motion-JPEG2000 and the BPCS steganography process are presented. Furthermore, the 3-D SPIHT and the BPCS steganography process are evaluated. The simulation results proved that the 3-D SPIHT with BPCS steganography achieved better performance than the Motion-JPEG2000 and BPCS steganography.

Mansouri et al. [29] suggested an adaptive steganography scheme based on spatial and temporal features of the human visual system and video signal features to hide secret information in a coded video sequence. The motion vectors of the P-VOP (Video Object Plane), B-VOP, and qualified-DCT coefficients of I-VOP are utilized for the spatial and temporal characteristics of the video, respectively. The extraction of the hidden data is performed without full decompression. The simulation outcomes proved that the suggested adaptive steganography method has high capacity and imperceptibility. Dasgupta et al. [4] developed a video steganography algorithm for hiding the secret data in video frames based on the LSB method. The proposed algorithm is improved by utilizing the genetic algorithm that is developed to obtain an optimum embedded message imperceptibility. Video quality and imperceptibility are the main factors to measure the efficiency and effectiveness of secret data hiding and extraction. The tests and findings proved that the suggested algorithm improved the image fidelity and PSNR.

Ramalingam et al. [41] offered a video steganography scheme based on a Markov model to enhance the embedding and extraction speed of the embedded message. They utilized the state transition dynamics and the conditional states among the video frames to hide and extract the secret message. The simulation results proved that the suggested algorithm improved the information embedding time by 3–50%, the extraction rate of secret message enhanced by 21–76%, with a processing computational cost of 21–90%, and the protection performance enhanced by 5–76% compared to the literature algorithms. Mihara et al. [32] presented a quantum steganography approach based on prior entanglement, where it depends on quantum physics. This approach is based on combining the quantum error-correcting codes and prior entanglement that allows the hidden message and cover message content to be created,

separately. In several steganography methods, hiding a secret message in error-correcting codes may give rise to harm if the hidden region is corrupted. The proposed approach considered that the essential cover message form must not be changed due to the hidden message.

Sushmitha et al. [48] developed a proposed video steganography system to hide a video as a secret data in another video stream as a cover data based on the DWT. Also, the authors extended the proposed system to embed double-secret videos in one cover video. The experimental outcomes achieved acceptable PSNR with negligible degradation in video quality and the difference amongst the original video, stage-video, and reconstructed secret video is not noticeable. Khalil et al. [19] presented an efficient technique for embedding audio samples in the digital image quaternion frequency domain. Each sample of the employed audio signal is integrated with the pixel values of the three-color components attended from the utilized cover digital image to yield a quaternion number. The absolute value of this quaternion number is communicated, and then the original sample of the audio signal is obtained at the receiver based on simple quaternion mathematics. Ramadhan et al. [33] suggested a secure and robust HEVC steganography method based on error-correcting codes and multiple object tracking (MOT) algorithm in the DCT and DWT domains. The secret message is firstly encoded and subsequently inserted into the coefficients of the DCT and DWT of the regions of interest of the host HEVC frames. The outcomes demonstrated that the suggested scheme increased the imperceptibility, embedding capacity, and security performance against different attacks.

Khalil et al. [20] suggested a steganography methodology depending on the quaternion Fourier transform to conceal text information in a digital cover electronic image. The secret information is transferred to the quaternion domain before its embedding, and the digital cover electronic image is represented in the quaternion domain space. The simulation results proved that the embedded message is extracted without changes from the original message and the cover image can be transmitted without noticeable changes. Hashemzadeh et al. [10] suggested a video steganography scheme based on the human visual system's weaknesses to understand the modifications in dynamic scenes. The algorithm depends on detecting video scene regions with extremely dynamic. Then, it utilizes these regions to embed the data and computes the data size that will be hidden in detecting dynamic regions. The scene dynamics are determined by utilizing the motion clues of feature points, and the capacity of each hidden pixel is determined by statistical indicators based on the feature points behaviors. The simulation outcomes demonstrated that the proposed scheme achieved acceptable execution than the existing algorithms.

Wang et al. [52] introduced an improved intra-prediction mode (IPM)-based HEVC steganography scheme. The security efficiency of stego HEVC frames is achieved by embedding secret messages in the coding and prediction units of the compressed video frames. Simulation results clarified that the presented scheme could be implemented easily, and it could maintain the video quality. Shuyang et al. [27] presented a robust secret sharing based HEVC steganography algorithm. In the proposed algorithm, three different intra-frame prediction classes are utilized to avoid the distortion drift of the HEVC intra-frames. In the proposed algorithm, the embedded data has been coded into various sub-secrets to enhance the robustness performance of the secret message. After that, the encoded data is inserted into the frequency coefficient values of the luminance blocks of the HEVC frames. The simulation outcomes proved the survival of the proposed algorithm against attacks compared to the literature algorithms. Dong et al. [5] suggested an efficient HEVC steganography scheme based on small-sized Prediction Blocks (PBs) and large-sized PBs. The proposed technique exploits the feature of multi-sized prediction modes in the HEVC coding to perform the

steganography process. The advantages of the proposed technique are the enhancement of embedding capacity and the preservation of coding efficiency.

Zhe et al. [24] studied an efficient HEVC steganography methodology that transmits video frames with great privacy. The proposed steganography scheme is depending on the DCT domain and chaotic logistic mapping to improve video privacy and protection. Mehmet et al. [22] presented an effective HEVC hiding technique with achieving higher levels of capacity and fidelity. The proposed data hiding scheme is depending on the matrix coding scheme that embeds the secret data into the discrete sine frequency coefficient of the high-efficiency video encoded frames. Also, the proposed technique avoids error propagation resulted from the embedding process to achieve minimum distortion level in the visual quality of the transmitted HEVC frames. Galiano et al. [7] suggested an HEVC hiding approach based on changing the luminance video frame-blocks to embed and recover the secret data in HEVC frames. Simulation results proved that the proposed hiding scheme could recover secret information, maintain good visual quality, and robust to most of the steganalysis attacks.

The greatest critical and main disadvantages established in the related steganography techniques that will be avoided in our proposed QFFT-based HEVC steganography approach are as follows:

- Many of the related techniques are uniquely and barely based on the original secret message without any pre-processing stages such as compression or encryption.
- Many of the related techniques have not introduced a significant accomplishment for the estimated evaluation metrics like PSNR, SSIM, FSIM, and correlation coefficient.
- Many of the related techniques failed to recover the secret message at the receiver side.
- Many of the related techniques employ extremely two or three test digital images or videos for assessments and evaluations.
- Many of the related techniques have not studied more steganalysis attacks on the stego videos.
- Many of the related techniques have not studied the effect of noise attack on the stego videos to professionally evaluate the performance efficiency of the presented algorithm.
- Many of the related techniques presented high computational cost or the time processing of the steganography process is not considered.
- Many of the related techniques have not studied widespread comparisons with the previous related works.

Due to the practical and academic importance of HEVC security in different multimedia applications, we are motivated to introduce an efficient HEVC steganography method. Also, in terms of development with considering the restrictions of the literature algorithms, this motivated us to propose a covert HEVC steganography scheme in this paper to study the possibility of hiding an encrypted secret audio message within the stego HEVC frames in a complicated and secure manner. Moreover, to enable this scheme to be contrasted with the literature approaches, the main contribution of the suggested HEVC steganography scheme that it hides a large quantity of secret information with achieving higher robustness against multimedia steganalysis contrasted to the previous approaches. Also, the suggested scheme ensures that the secret information will be unobserved from intrusions attempts on the cover HEVC frames. Therefore, instead of direct hiding the plain audio message within the stego-media, the proposed approach applies two consecutive layers of encryption to the plain audio message before embedding it within the video signal. The first encryption layer is performed

using the random projection encryption based on the Legendre sequence in the DWT domain. In the second encryption layer, the yielded audio message is represented as quaternion numbers using the QFFT technique. In the embedding process, the quaternion mathematics is employed to transfer HEVC video frames to the quaternion format to embrace the secret data which is also characterized in the quaternion domain.

Thus, the major novelty of this work is the introduction of an effective HEVC video steganography approach to hide a block of compressed and encrypted audio data within HEVC frames by using the quaternion mathematics concepts and QFFT. Firstly, the quaternion information is switched to the frequency domain utilizing the QFFT technique, and each cover video frame is converted to a quaternion form. The proposed approach can hide a large amount of secret audio information into the HEVC video frames with achieving higher imperceptibility. Also, at the receiver, the hidden secret audio information can be extracted utilizing straightforward quaternion functions and mathematics. The suggested approach has more robustness performance against the trails of multimedia steganalysis contrasted to the previous approaches. This article is structured as follows. Section 2 presents the basics of the related concepts used in this paper. The proposed HEVC video steganography approach is introduced in section 3. Section 4 provides the simulation outcomes and comparison analyses to evaluate the performance of the suggested steganography scheme. Section 5 concludes the paper and recommends some future works.

2 Preliminaries related work

In this section, the basic concepts of the DWT, random projection process, Legendre sequences, DCT-based compression process, and the concepts of quaternion mathematics used in this paper are discussed.

2.1 Basics of the DWT

The DWT can be utilized for the multiresolution decomposition process of a speech signal. It decomposes a given audio signal of a length (L) into two different sub-bands of different scales with a length ($L/2$) to investigate each scale, independently. The multiresolution output of the DWT can be described as the detail and approximation coefficients that have high-frequency components and low-frequency components, respectively. The approximation coefficients are generated by means of passing the speech signal through a low-pass filter, while the detail coefficients are generated by passing the speech signal through a high-pass filter. These coefficients can be utilized to build the model of the speech and audio signals [26]. The wavelet process can be represented as given in Fig. 1. In this paper, the DWT is employed to convert the input speech signal from a spatial pixel domain to a transform domain. Then, an encryption process is introduced to the obtained coefficients that considered as a diffusion process. The encryption process can be accomplished by changing the values (diffusion) or positions of the coefficients (permutation) to provide more confidentiality.

The two filters outputs can be described as follows [46]:

$$y_{low}[n] = \sum_{k=-\infty}^{\infty} x[k]\, h[2n-k] \tag{1}$$

$$y_{high}[n] = \sum_{k=-\infty}^{\infty} x[k]\, g[2n-k] \tag{2}$$

where $x[k]$ is the input speech signal, and $g[n]$ and $h(n)$ are the impulse functions of the high pass filter and low pass filter, consistently.

2.2 Basics of random projection process

It is known that the main objective of any data transformation using the projection technique is to reserve the data with much information as possible between the original and the transformed data groups with achieving better representation of the data in its new pattern. Random projection is introduced to project data points to random directions that are independent of the dataset [31]. It can be considered as a local sensitivity hashing method that is used for data hiding and security applications [35, 37].

The random projection process can be obtained by projecting the original signal on a random space [17, 38]. It can be generated by multiplication the original signal with a random matrix. It can be expressed as in (3):

$$\overrightarrow{\mathbf{Y}}_{k*n} = \mathbf{A}_{k*d}\, \overrightarrow{\mathbf{X}}_{d*N} \tag{3}$$

where $\mathbf{Y}$ and $\mathbf{X}$ represent the output and input random vectors, respectively. The vector $\mathbf{A}$ represents the random matrix.

It is worth mentioning that random projection retains the distance between the original and the produced data points with a high probability. It is proved in [31] that

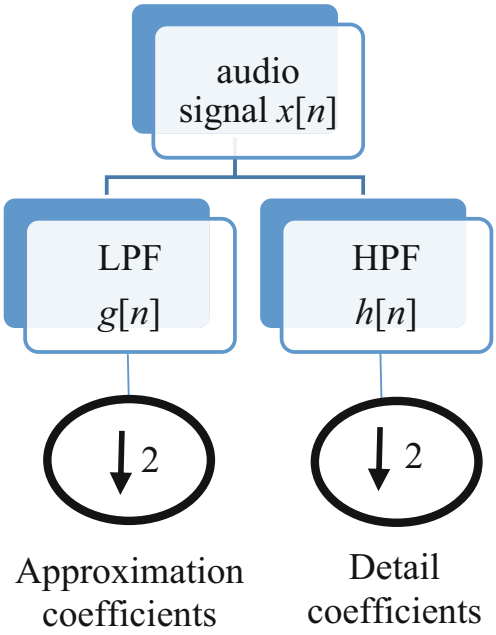


Fig. 1 Concept of the wavelet analysis

the required distances in the random space can be obtained using Gaussian random matrices. In this paper, the random matrix can be attained using Legendre sequences. Therefore, the proposed HEVC steganography system will be more robust against attacks.

2.3 Basics of Legendre sequences

Legendre sequences are also called pseudorandom sequences are generated using a deterministic algorithm. The Legendre and Pseudorandom sequences have broad applications in several disciplines like keystream sequences in stream ciphers, communication systems, computer simulation, cryptography, steganography, and other communication areas. Pseudorandom sequences are required to satisfy several randomness properties; otherwise, attacks can be launched based on the statistical deviation between the pseudorandom sequences and truly random sequences. In [8], the authors proposed three axioms for the appearance of binary periodic pseudorandom sequences: balanced, run property, and ideal autocorrelation. A pseudorandom sequence generator should have the following characteristics: good randomness of output sequences, long period, speed and efficiency, reproducibility, easy to implement, and fast computation.

For a prime $p > 2$, let S_n be the Legendre sequence that is defined as [8, 53]:

$$S_n = \begin{cases} 1, & \left(\frac{n}{p}\right) = -1, \\ 0, & Otherwise, \end{cases} \qquad n \geq 0 \tag{4}$$

where $\left(\frac{n}{p}\right)$ denotes the Legendre symbol.

The Legendre sequence is a binary structure with many interesting randomness properties, ideal periodic, aperiodic autocorrelation functions, and large linear complexity. The linear complexity established with the common Berlekamp-Massey method [8]. The Legendre sequence has a great linear-complexity named the linear k-error complexity which does not decrease by any alterations in its initial conditions. So, this motivated us to employ the Legendre sequence in our proposed algorithm for encryption process due to its significant features. The linear complexity of a Legendre sequence is determined in [53].

2.4 Basics of DCT-based compression algorithm

Data compression is an approach that is employed to decrease the data size required to represent the sampled digital data, and therefore, it decreases the storage cost and transmission rate. Compression types are lossless and lossy compression [42]. In lossless coding approaches, the original information can be completely retrieved from the encoded (compressed) data. In lossy compression approaches, the retrieved data from the compressed data is not completely identical to the original data. The most utilized lossy compression approaches are based on the DCT, which is an algorithm that is used to convert a signal into primary frequency components. The DCT is widely utilized in image compression applications, and it is a close respective to the Discrete Fourier Transform (DFT). Based on the compression process, the DCT achieves better performance than the DFT, where it converges the low frequencies which include useful data in the upper left block corner. The DCT

quantization based on maintaining the low frequencies and zeroing further entries. So, due to the considerable advantage of the DCT, this motivated us to employ it in our proposed algorithm for compression process.

During the encoding process, different processes such as zig-zag scanning, quantization, variable-length encoding, and run-length-encoding are applied after the DCT. This process flow is inverted during the decoding process. In this work, we employed the DCT-based compression algorithm to compress the audio signal, where the audio signal is converted to a square matrix before applying the compression process. The proposed DCT-based compression approach utilizes different quantization matrices of DCT's coefficients, and the determined level of quantization matrix is concerning to the standard deviation of DCT's coefficient blocks.

2.5 Basics of quaternion definition and algebras

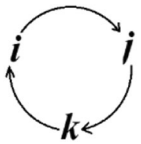
Hamilton discovered a way to multiply in four dimensions, not three [9]. It is called a Quaternion, which has four components: three imaginary and one real. The elements of $\mathbb{H}$ for the real quaternions are given as follows:

$$\mathbb{H} = \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\} \tag{5}$$

where $\mathbb{H}$ as a 4-dimensional vector space over $\mathbb{R}$, $\mathbb{R}$ is the field of real numbers, the set $\{1, i, j, k\}$ is a natural basis for $\mathbb{H}$ vector space, and the following rules are imposed:

$$\begin{array}{c} i^2 = j^2 = k^2 = ijk = -1 \\ ij = k, \quad jk = i, \quad ki = j \\ ji = -k, \quad kj = -i, ik = -j \end{array} \tag{6}$$

The rules for multiplying i, j, and k by each other, put them in alphabetical order around a circle as explained in [12].



The products which are following clockwise get a positive sign and products which are going against the order get a negative sign, e.g., $ki = j$ and $ik = -j$. For a quaternion,

$$q = a + bi + cj + dk \quad \in \mathbb{H} \tag{7}$$

and its conjugate $\overline{q}$ is defined to be,

$$\overline{q} = a - bi - cj - dk \quad \in \mathbb{H} \tag{8}$$

which has the properties of: $\overline{q_1 + q_2} = \overline{q_1} + \overline{q_2}$, $\overline{q_1}\ q_2 = \overline{q_1}\,\overline{q_2}$, $\overline{\overline{q}} = q$. The norm of q is given as follows.

$$N(q) = a^2 + b^2 + c^2 + d^2 \tag{9}$$

Then, the $\overline{q}q = q\overline{q}$ and $N(q_1 q_2) = q_1 q_2 \overline{q_1 q_2} = q_1 q_2 \overline{q_2}\,\overline{q}_1 = q_1 N(q_2)\,\overline{q}_1 = q_1\,\overline{q}_1 N(q_2) = N(q_{21})N(q_2)$. The imaginary and real components of q are defined as:

$Im(q) = bi + cj + dk \in \mathbb{I}$ and $Re(q) = a \in \mathbb{R}$.If $q \neq 0$, then, the inverse of $q \neq \mathrm{H}$ is given as follows.

$$q^{-1} = \frac{\widetilde{q}}{|q^2|} \tag{10}$$

A pure quaternion can be defined as a quaternion with zero real part, while a unit quaternion can be represented as a quaternion with unit modulus.

$$q = \frac{i + j + k}{\sqrt{3}} \tag{11}$$

The quaternion imaginary quantity can be expressed as three components that can be represented graphically in a three-space vector. Therefore, the quaternion number q can be explained as a summation of two parts: a scalar part $S(q)$ and a vector part $\mathbf{V}(q)$ as follows:

$$q = S(q) + \mathbf{V}(q) \tag{12}$$

where $\mathbf{V}(q)$ is a composition of three imaginary components:

$$\boldsymbol{V}(q) = bi + cj + dk \tag{13}$$

and $S(q)$ is the real components ($S(q) = a$).

The Discrete Quaternion Fourier transforms (DQFT) has been defined in [12]. There are three different types of the DQFT which are the two-sides DQFT, the left-side DQFT, and the right-side DQFT. These types are established according to the quaternion noncommutative property of the quaternion. Besides, they can be mathematically represented as follows [12]:

1. The two-sides DQFT:

$$F_{L-R}(u,v) = \frac{1}{\sqrt{MN}} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} e^{-\mu 2\pi \frac{xu}{M}} f(x,y) e^{-\mu 2\pi \frac{vy}{N}} \tag{14}$$

2. The left-side DQFT:

$$F_L(u,v) = \frac{1}{\sqrt{MN}} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} e^{-\mu 2\pi \left(\frac{xu}{M} + \frac{vy}{N}\right)} f(x,y) \tag{15}$$

3. The right-side DQFT:

$$F_R(u,v) = \frac{1}{\sqrt{MN}} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x,y)\ e^{-\mu 2\pi \left(\frac{xu}{M} + \frac{vy}{N}\right)} \tag{16}$$

where μ is a unit of any pure quaternion.

$$F_f^{-q}\left[F_f^q\right](m,n) = f(m,n) = \frac{1}{MN} \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} F_f^q(u,v) e^{\mu 2\pi \left(\frac{mu}{M} + \frac{nv}{N}\right)} \tag{17}$$

The Inverse Discrete Quaternion Fourier Transforms (IDQFT) can be represented mathematically as follows [12]:

1. The two-sides IDQFT:

$$f(x,y) = \frac{1}{\sqrt{MN}} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} e^{\mu 2\pi \frac{xu}{M}} F_{L-R}(u,v) e^{\mu 2\pi \frac{yv}{N}} \tag{18}$$

2. The left-side IDQFT:

$$f(x,y) = \frac{1}{\sqrt{MN}} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} e^{\mu 2\pi \left(\frac{xu}{M} + \frac{yv}{N}\right)} F_L(u,v) \tag{19}$$

3. The right-side IDQFT:

$$f(x,y) = \frac{1}{\sqrt{MN}} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} F_R(u,v) \; e^{\mu 2\pi \left(\frac{xu}{M} + \frac{yv}{N}\right)} \tag{20}$$

The color image pixel or color video frame can be denoted as a pure quaternion if it requires a representation as a quaternion form [18]. It has three components of Blue, Green, and Red (RGB). The imaginary parts of a pure quaternion can be used to represent the RGB components. A pixel at image coordinates $f(x, y)$ in an RGB digital image can be expressed as follows:

$$f(x,y) = 0a + Ri + Gj + B\mathrm{k} \tag{21}$$

where B, R, and G are blue, red, and green parts of a color digital image, correspondingly. For more details, descriptions, and explanations concerning the above-mentioned equations and their terminologies can be found in [9, 12, 18].

3 Proposed QFFT-based HEVC steganography approach

The proposed QFFT-based HEVC steganography approach comprises of two main processes. The first one is for hiding a secret audio message within the stego video frame (the cover after embedding the secret information), and the second one is for obtaining the hidden audio message. The embedding procedure is utilized to hide an encrypted secret audio message within the cover video frames. It is important to be insured the unnoticeability of the secret information from intruders' interceptions on the cover HEVC frames. The extraction procedure is employed to reconstruct and extract the hidden secret information at the receiver side without any distortion with good quality. To assure that the proposed approach comprises of both high payload and high security, efficient cryptographic and compression techniques are employed as pre-processing steps on the secret audio message.

3.1 Proposed embedding procedure

The flow diagram of the whole embedding procedure of the proposed QFFT-based HEVC steganography approach is introduced in Fig. 2. The embedding procedure requires two main inputs: the first input is the secret audio message and the second input is the cover HEVC frame. The cover HEVC video frames are used to be the stego media that will contain a secret audio message. Each input video frame is resized into a square frame with a height h and a width w, and it is called a stego video frame. So, the secret audio message that will be hidden and embedded into the

cover video frames must have not a maximum length greater than the value of $L = h \times w = h^2$. So, to embed a high amount of audio data in a stego cover, the transmitted audio message can be compressed prior to the process of embedding. In this paper, the DCT-based compression method is employed for compressing the audio signal. The audio signal is converted to a square matrix before applying the DCT-based compression technique that is based on various quantization matrices of DCT's coefficients.

To ensure that the suggested steganography scheme is more complicated against steganalysis, the compressed message (audio signal) is encrypted prior to embedding it into the cover video frame using a random projection algorithm based on the Legendre sequence. The schematic description of the proposed encryption process is illustrated in Fig. 3. It consists of two stages: the DWT analysis stage and the random projection encryption stage. In the DWT analysis phase, the secret audio information is decomposed into two sub-signals using the DWT to convert the input audio signal from the time domain to the transform domain. The two sub-bands are the approximation and details coefficients. The second stage is established using the random projection of the wavelet coefficients. The random matrix used in the random projection process is generated using the Legendre sequence that is a pseudo-random noise binary sequence used as a key for the encryption process. It is a semi-random sequence in the sense that it seems random within the sequence length, and it satisfies the randomness needs. Regarding the number of coefficients in each sub-band, the Legendre matrix is produced from a set of prime numbers. This matrix consists of a sequence that is repeated to create the required length. This sequence is exploited for encrypting the approximation and details coefficients, separately. The secret audio signal is generated by the concatenation of the two wavelet coefficients; therefore, the secret audio message has the same length as the original audio message.

At the receiver, the original audio secret information can be reconstructed by partitioning the secret audio message into two parts, and the inverse random projection transform is applied to each part, separately. Then, the inverse DWT is employed to reconstruct the compressed audio message. Finally, the decompression is applied to this signal to recover the original audio signal.

The stego HEVC frame is separated into the G, R, and B (green, red, and blue) elements that are utilized to build quaternion numbers Q_A in the form of a square array with the zero-real component:

$$Q_A = 0w + Ri + Gj + Bk \tag{22}$$

Based on the mathematical discussions introduced in section 2.5, a secret audio signal with a length $\leq L$ is obtained in the form of a string, and each character value (c) of the acquired string is utilized to put the real component in a quaternion array Q_S:

$$Q_S = cw + 0i + 0j + 0k \tag{23}$$

The quaternion Fourier transform of Q_S is computed as:

$$Q_B = QFFT(\, Q_S) = mw + xi + xj + xk \tag{24}$$

The magnitudes of the three vector parts of the generated Q_B are identical. From quaternion concepts, it is known that in the case of obtaining three vector parts of a quaternion array with magnitudes of zeros, therefore, the generated quaternion Fourier transform

of this such array will be in the manner demonstrated in Eq. (24). This is an important feature from the quaternion concepts that will be a considerable collaborator in building the embedding procedure, where it is potential to utilize only two elements of the quaternion array Q_B that are x and m.

The subsequent action is to insert the secret audio signal in the quaternion transform domain (Q_B) within the stego video frame in the quaternion arrangement (Q_A). For guaranteeing that the audio secret signal turns unobserved, a little percentage of Q_B is mixed to a great percentage of Q_A. To achieve this purpose, two factors γ and α are utilized with assuming that $\alpha + \gamma \cong 1$. Therefore, a small ratio of γ and a high ratio of α are employed to create the stego video frame as follows:

$$\begin{aligned} Q_T &= \alpha\,(0w + Ri + Gj + Bk) + \ \gamma\,(0w + mi + xj + 0k) \\ Q_T &= 0w + (\,\alpha\,R + \gamma\,\mathrm{m})\,i + (\,\alpha\,G + \gamma\,x)\,j + \ \alpha\,B \end{aligned} \tag{25}$$

The array that is introduced in Eq. (25) signifies the resulted stego HEVC frame, and it is communicated through an insecure or a secure communication channel. The

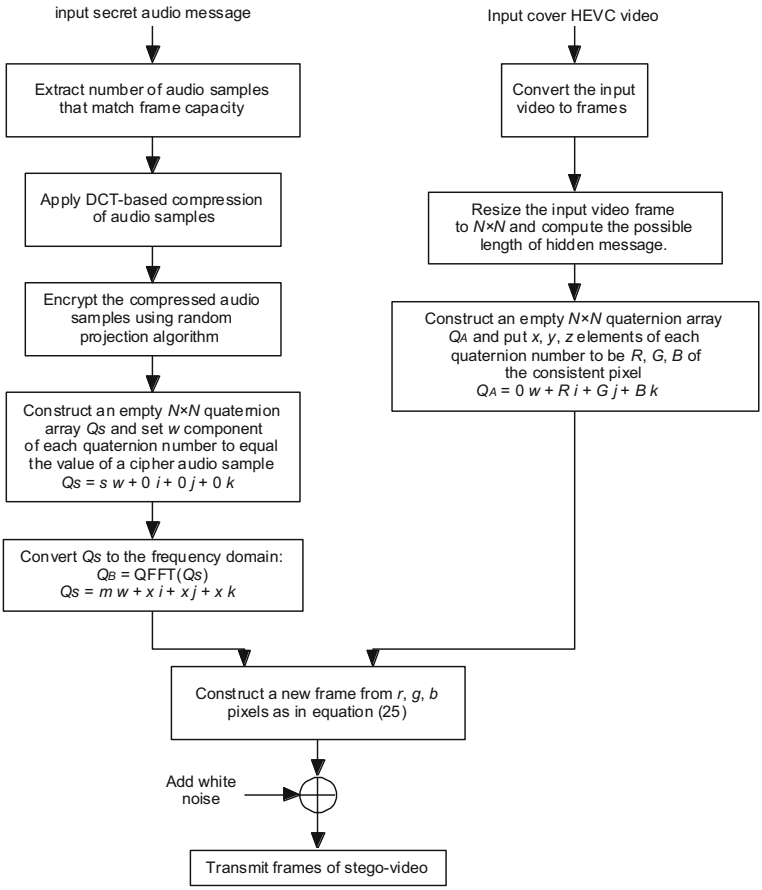


Fig. 2 The flow diagram of the embedding procedure of the suggested steganography approach

pseudocode description of the suggested embedding procedure is demonstrated in Algorithm (1).

Algorithm (1) The pseudocode description of the suggested embedding procedure.

// input α , γ
// get cover HEVC video frame
// get secret compressed-encrypted audio message
// resize the input video frame to be in square dimensions
// construct quaternion array Q_A form pixels for each pixel $p_{i,j}$ in the cover video frame
{
$R_{i,j}, G_{i,j}, B_{i,j} \leftarrow p_{i,j}$
$Q_A(i,j) \leftarrow 0\,w + Rr_{i,j}\,i + G_{i,j}\,j + B_{i,j}\,k$
}
// construct a quaternion array Q_S form secret message
for each character c_n in the secret message
{
$Q_S(i,j) \leftarrow c_n w + 0\,i + 0\,j + 0\,k$
}
// convert Q_S to a quaternion fast Fourier transform
$Q_B \leftarrow QFFFT(Q_S)$
Q_B (takes the form) $\equiv m\,w + x\,i + x\,j + x\,k$
$Q_T \leftarrow \alpha(0w + Ri + Gj + Bk) + \gamma(m\,w + x\,i + x\,j + x\,k)$
$r \leftarrow \alpha R + \gamma\ m$
$g \leftarrow \alpha G + \gamma\ x$
$b \leftarrow \alpha B$
Transmit a stego video frame $f(r, g, b)$

3.2 Proposed extraction procedure

The schematic flow diagram of the extraction procedure is displayed in Fig. 4. This procedure requires two inputs for recovering the secret audio message. These inputs are the received stego HEVC video and the original HEVC video. As described in the preceding discussion that the original HEVC frame must be resized and subsequently characterized in the form of a quaternion array as in (26).

$$Q_A = 0w + Ri + Gj + Bk \tag{26}$$

The received stego video frame is resized, and then characterized in a quaternion structure as:

$$Q_a = 0w + r'i + g'j + b'k \tag{27}$$

For providing the values of γ and α with utilizing Eqs. (24) and (25), the secret audio signal information can be calculated as:

$$m' = (r' - \alpha R)/\gamma \tag{28}$$

$$x' = (g' - \alpha G)/\gamma \tag{29}$$

$$Q_f = m' + x'i + x'j + x'k \tag{30}$$

The inverse process of the QFFT of Q_f produced:

$$Q_{c'} = IQFFT\left(Q_f\right) = S'w + 0\,i + 0\,j + 0\,k \tag{31}$$

where the obtained and reconstructed secret audio data is given by S'. The pseudocode description of the suggested extraction procedure is demonstrated in Algorithm (2).

Algorithm (2) The pseudocode description of the suggested extraction procedure.

// input α , γ
// get original video frame $I(R, G, B)$
$Q_A = 0w + Ri + Gj + Bk$
// get received video frame $f(r', g', b')$
$Q_a = 0w + r'i + g'j + b'k$
$m' \leftarrow (r' - \alpha R) / \gamma$
$x' \leftarrow (g' - \alpha G) / \gamma$
// construct a quaternion array
$Q_f \leftarrow m' + x'i + x'j + x'k$
// get the inverse quaternion fast Fourier transform
$Qc' \leftarrow IQFFT\ (Q_f)$
$Q_{c'}$ (will be in the form) $\equiv S'w + 0\,i + 0\,j + 0\,k$
The extracted secret compressed-encrypted message = S'

4 Simulation results and comparative analysis

In the previous section, an efficient approach is suggested for concealing secret data (audio signal) within cover HEVC video frames. The identical approach can be employed to conceal a text or an image within cover HEVC frames. Firstly, the implementation of HEVC coding scheme is performed to compress the transferred HEVC sequences owing to its efficient coding and decoding performance. Numerous examinations and analyses on various HEVC test sequences, e.g., Balloons, Basketball, Breakdancer, PoznanHall, and Uli [34]. The utilized HEVC video sequences have different spatial and temporal characteristics. The standard of the H.265/HEVC

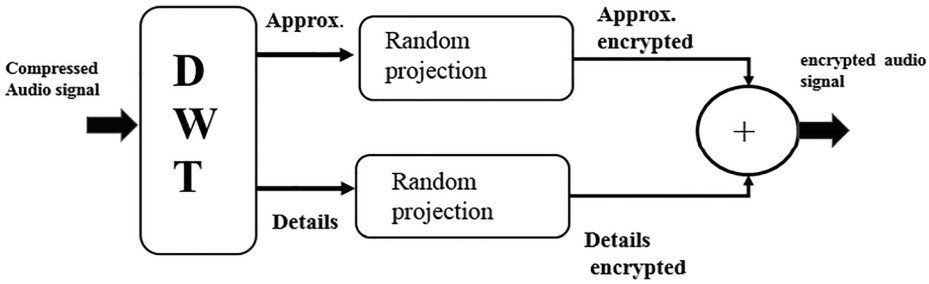


Fig. 3 The description of suggested encryption algorithm

Test Model (HM) codec [11] is employed to generate the compressed HEVC frames of each tested stream. After that, the simulation results are carried out on Intel Core i7–3770@2.80GHz with 16GB RAM using windows 10 64-bit running system utilizing MATLAB R2019b software to test and evaluate the proposed QFFT-based HEVC steganography approach.

Therefore, the suggested HEVC hiding approach is consisting of two fundamental processes: the first one is the embedding process and the second one is the extraction process. The embedding procedure is utilized to hide a secret audio signal inside a cover compressed HEVC video frame. The extraction process leads to revealing the secret audio signal at the receiver side. The MATLAB functions are employed to build the mathematical quaternion model to represent the compressed HEVC video frame and the secret encrypted-compressed audio message in quaternion arrays form. Both IQFFT and QFFT operations have been exploited

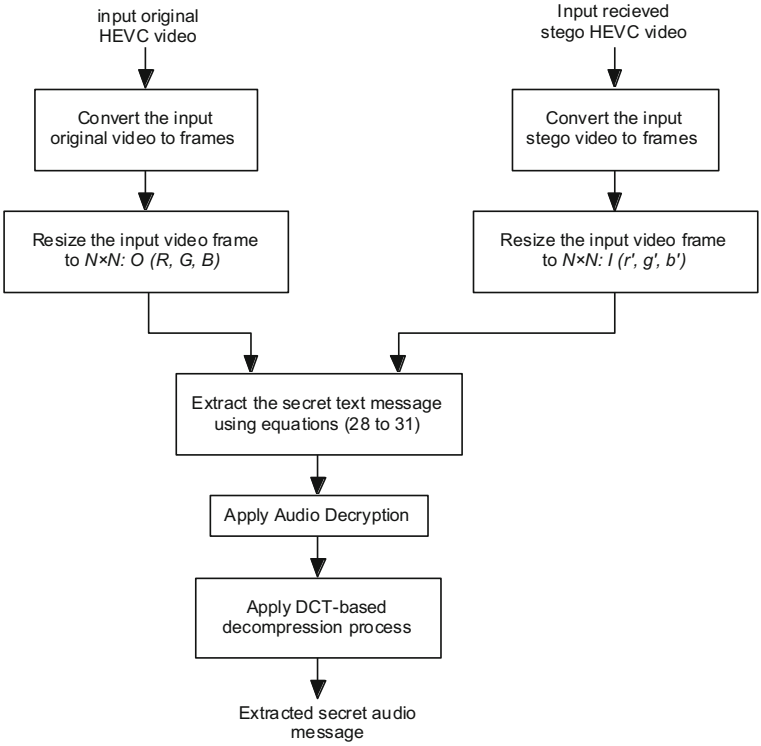


Fig. 4 The flow diagram of the extraction procedure of the suggested steganography approach

for transforming from the spatial to the frequency domain and for the contrariwise process. These operations produce real numbers and values in the quaternion form.

One of the most important properties for any proposed steganography algorithm is the amount of concealing capacity. It is the greatest data that can be securely inserted in the cover medium with no noticing statistically perceptible things and robustness, which refers to how well the steganographic algorithm resists the extraction of hidden data. Considering the proposed QFFT-based steganography approach of embedding audio signal within the cover HEVC frames: the number of hidden audio samples depends on the number of pixels of a cover video frame. Assuming a video frame of $W \times H$ dimensions, where $H \leq W$, the number of 8-bit audio samples that can be hidden within one video frame is H^2. This amount of hidden data is higher than that of the traditional LSB scheme in which the data is embedded only in the least significant bit of each pixel for the same video frame, this amount equals to $3H \times W/8$.

To confirm the success and robustness of the proposed encryption scheme in addition to the proposed steganography approach, the quality of encrypted, compressed, and decrypted audio secret signals is investigated in our simulation tests. Fig. 5 (a and b) illustrates the time domain and the spectrogram results of two different tested long and short audio signals with different sizes (160Kilobyte and 35Kilobyte, respectively). It is known that the spectrogram is a graph of the intensity of a signal expressed as a function of frequency and time in which the vertical direction is the frequency (f), the horizontal direction is the time (t), and the amplitude (A) is shown on a grey-scale. It provides an exciting way to edit audio as it appears in tandem with a waveform display. The DCT-based compressed audio signals and their spectrograms of the employed long and short audio signals are presented in Fig. 6, while their ciphering audio patterns and their spectrograms are illustrated in Fig. 7. These encrypted audio signals are embedded into the cover video frames to form the stego video frames. It is obvious from spectrograms that the ciphered audio signals are similar to the white noise, therefore any intelligibility of the audio signals is removed. At the receiver side, the audio signals are extracted and reconstructed. Fig. 8 shows the reconstructed (deciphered and decompressed) audio signals and their spectrograms for the long and short audio signals.

The accuracy of the residual intelligibility is utilized to assess the perceptual and visual quality of the ciphered and deciphered audio signals. To demonstrate the robustness of the residual intelligibility, the objective qualities are measured that include the spectral and time domains metrics. The first one of time-domain metrics incorporates Signal-to-Noise Ratio (SNR) and Segmental SNR (SNRseg). The second one of the spectral domain metrics includes Spectral Distortion (SD). The SNR is a relation amongst the signal and noise energy stated in decibels (dB) for the number of samples i, and it is given as follows [15]:

$$SNR = 10\log_{10} \frac{\sum_{i=1}^{N} x^2(i)}{\sum_{i=1}^{N} (x(i)-y(i))^2} \tag{32}$$

where $x(i)$ is the input original audio samples, and $y(i)$ is the output extracted audio samples. It is noticed that the SNR is simple in its calculation, but it is very sensitive to the time alignment of the original and processed audio signals. To achieve a better quality of the audio signals, the

SNR should record smaller values between the original and ciphered signals, while it should record higher values between the original and deciphered signals.

The SNRseg determines the average value of the *SNR* that is calculated over sequences of short frames for the audio signal with a total number of *M* and each frame that has a length of *N* that can be chosen between 15 and 20 msec. It can be estimated as follows [50]:

$$SNR_{seg} = \frac{10}{M}\sum_{m=0}^{M-1} log_{10}\frac{\sum_{n=Nm}^{Nm+N-1} x(n)^2}{\left(x(n)-\widehat{x}\,(n)\right)^2} \tag{33}$$

where $x(n)$ and $\widehat{x}\,(n)$ are the samples of the input original audio and the output processed audio signals, respectively. To achieve a better quality of the audio signals, the SNR_{seg} should record smaller values between the original and ciphered signals, while it should record higher values between the original and deciphered signals.

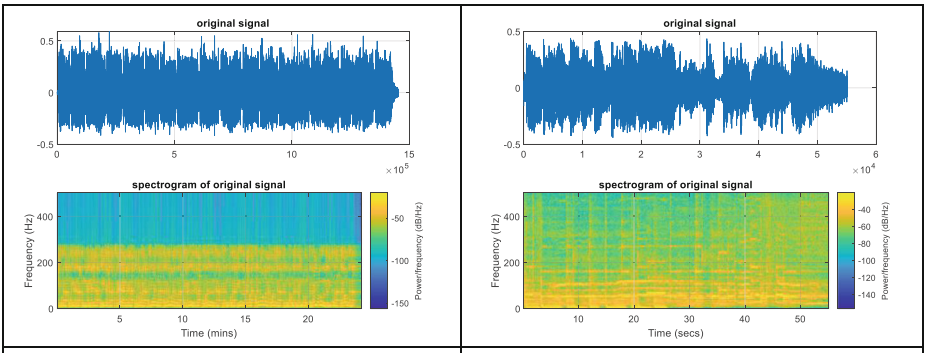
The *SD* term shows how the farness between the processed audio spectrum and the original one in the frequency domain. This measure is preferred compared to the time-domain measures because it is less influenced by possible time misalignments between the original and the processed audio signals. It can be calculated as follows [46]:

$$SD = \frac{1}{M}\sum_{m=0}^{M-1}\sum_{n=Nm}^{N-1}\left|V_x(n)-V_y(n)\right| \tag{34}$$

where $V_x(n)$ and $V_y(n)$ declare the original and the processed spectrum of the audio signal. To accomplish a superior performance and quality of the audio signals, the *SD* should record higher values between the original and ciphered signals, while it should record smaller values between the original and deciphered signals.

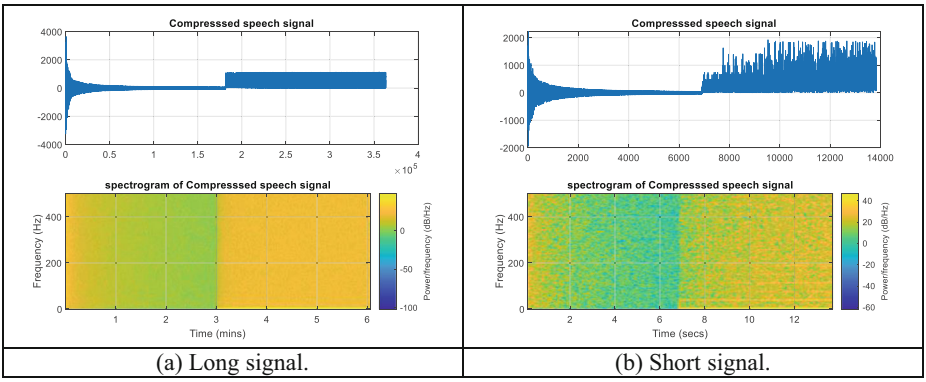
To validate the effective of the cryptosystem and the robustness of the proposed steganography approach, the correlation coefficient (r_{xy}) amongst the processed and the original signal samples is also measured that assess the quality of the proposed approach. It can be calculated by the following equation as defined in [46]:

$$r_{xy} = \frac{c_v(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{35}$$



(a) Long signal. (b) Short signal.

Fig. 5 The original audio signals and their spectrograms for the long and short signals



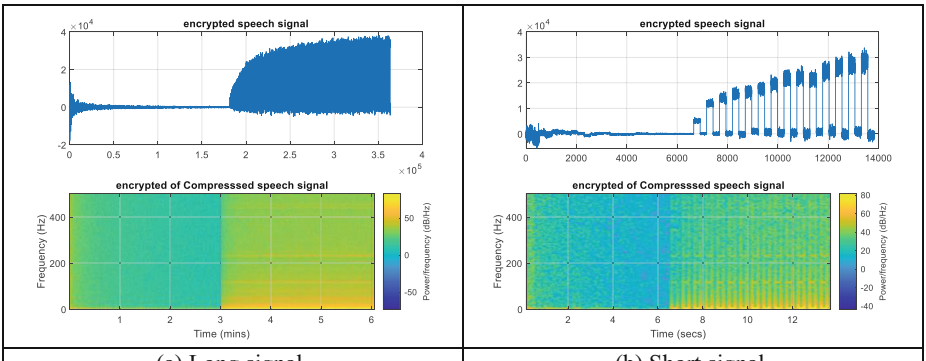
(a) Long signal. (b) Short signal.

Fig. 6 The compressed audio signals and their spectrograms for the long and short signals

where $c_v(x, y)$ is the covariance value amongst the original and processed audio signals. The $D(y)$ and $D(x)$ determine the variances values of the two audio signals y and x. To achieve a better quality of the audio signals, the r_{xy} should record smaller values between the original and ciphered signals, while it should record higher values between the original and deciphered signals.

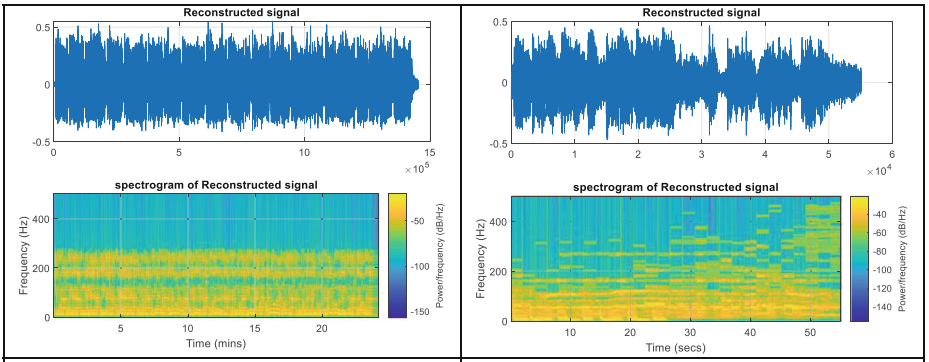
Further and more additional evaluation quality metrics are utilized to evaluate the effectiveness of the proposed cryptosystem and the robustness of the proposed steganography approach such as Number of Changing Pixel Rate (NPCR), Percent Root-mean-square Difference (PRD), Unified Averaged Changed Intensity (UACI), Perceptual Evaluation of Speech Quality (PESQ), Log-Likelihood Ratio (LLR), more details, explanations, and descriptions about these evaluation metrics can be found in [44, 45, 49]. Table 1 presents the *SNR*, SNR_{seg}, *SD*, LLR, PRD, PESQ, NPCR, UACI, and r_{xy} results of the employed two different long and short audio signals.

From Table 1, it is noticed that the *SNR* and SNR_{seg} of the ciphered audio messages have negative values, the r_{xy} values have smaller values less than one, and the values of the LLR, PRD, NPCR, UACI, and *SD* metrics have risen which reflects the great accomplishment of the proposed audio cryptosystem. The reconstructed audio signal at the receiver has low values of LLR, PRD, NPCR, UACI, and *SD* metrics and higher values of the PESQ, r_{xy}, *SNR*, and SNR_{seg}, this ensures high quality of the reconstructed signal. It is also observed that r_{xy} values



(a) Long signal. (b) Short signal.

Fig. 7 The ciphered audio signals and their spectrograms for the long and short signals



(a) Long signal. (b) Short signal.

Fig. 8 The reconstructed (deciphered and decompressed) audio signals and their spectrograms for the long and short signals

are near to one such that the decrypted audio signal is as the original reconstructed one, while the LLR, PRD, NPCR, UACI, and *SD* quantities have small values that imply high precision data and extremely good quality of the reconstructed audio signal. Therefore, it is obvious from the simulation outcomes that the suggested ciphering process utilized in our proposed steganography process is efficient and has superior privacy and robustness.

Referring to Eq. (25), two ratios of α and γ are used for hiding an audio message within video frames in a quaternion domain. The hiding and extraction processes are performed by varying α and γ to determine the adequate values for the embedding process. It is well known that robustness performance is an essential characteristic of efficient video hiding methods. So, the quality performance of the suggested steganography approach is studied and evaluated utilizing the different metrics of *PSNR*, *SSIM*, *FSIM*, and correlation coefficient. The *PSNR* can be measured by the following Eq. [28]:

$$PSNR = 10\log_{10}\frac{max_v}{MSE} \tag{36}$$

Table 1 The results of quality metrics of the ciphered long and short audio signals and the deciphered long and short audio signals

Quality metric	Ciphered audio signal		Deciphered audio signal	
	Long signal	Short signal	Long signal	Short signal
SNR (dB)	−29.96	−29.16	16.46	14.99
SD (dB)	56.20	53.28	2.85	3.48
SNR_{seg} (dB)	−29.97	−29.24	16.39	14.88
LLR (dB)	0.41	0.38	0.36	0.32
PRD (%)	7.43	7.39.71	0.15	0.11
PESQ	0.98	0.91	4.23	3.95
NPCR (%)	99.93	99.96	95.47	96.58
UACI (%)	33.37	33.34	28.63	29.31
r_{xy}	0.40	0.34	0.99	0.98

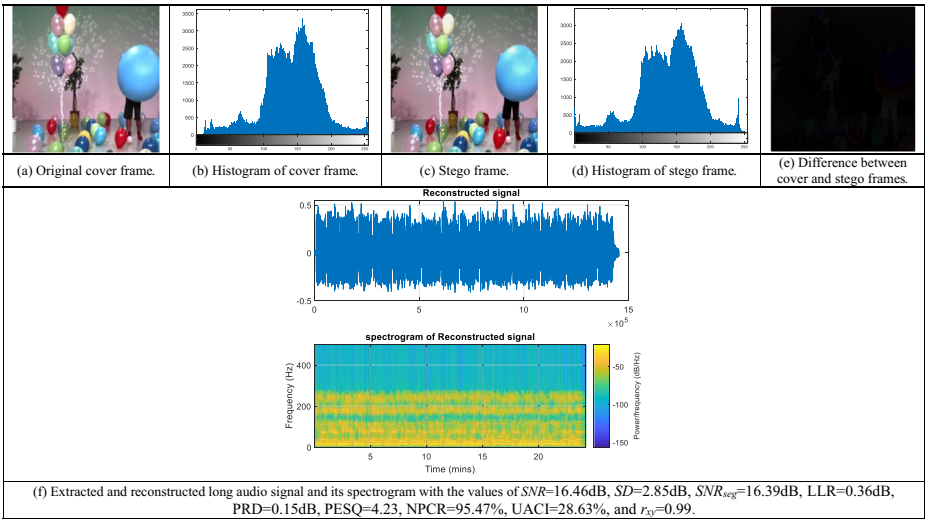


Fig. 9 The graphical results of the Balloons stream with the values of $PSNR = 31.25$ dB, $r_{xy} = 0.9969$, $SSIM = 0.9511$, $FSIM = 0.9883$, and processing time = 3.2 s in the case of using the long audio signal as a secret message

where max_y determines the highest pixel value of the video frame, and the value of mean square error (*MSE)* is calculated amongst the processed and the original video frames.

The *SSIM* is a measure for the similarity index between the stego and original video frames that can be defined as *y* and *x*, respectively [51]. The expression of the *SSIM* metric can be formulated as follows:

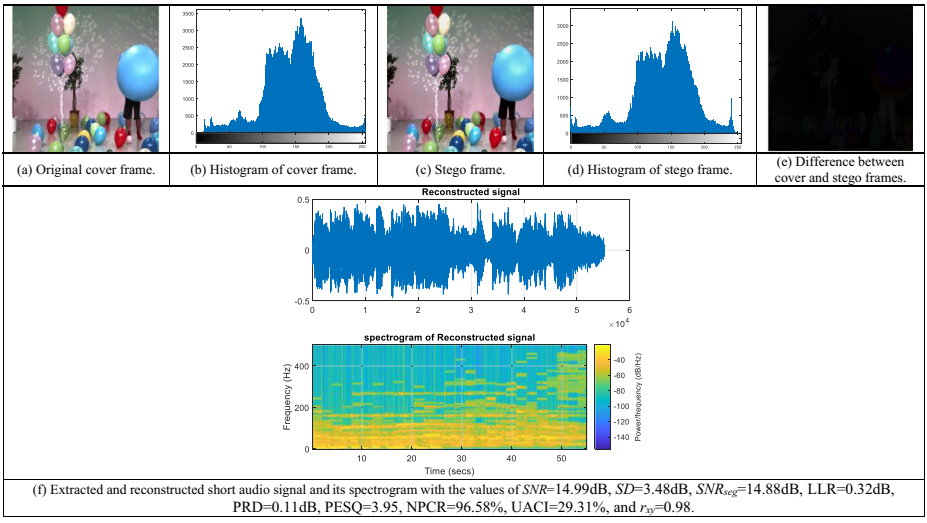
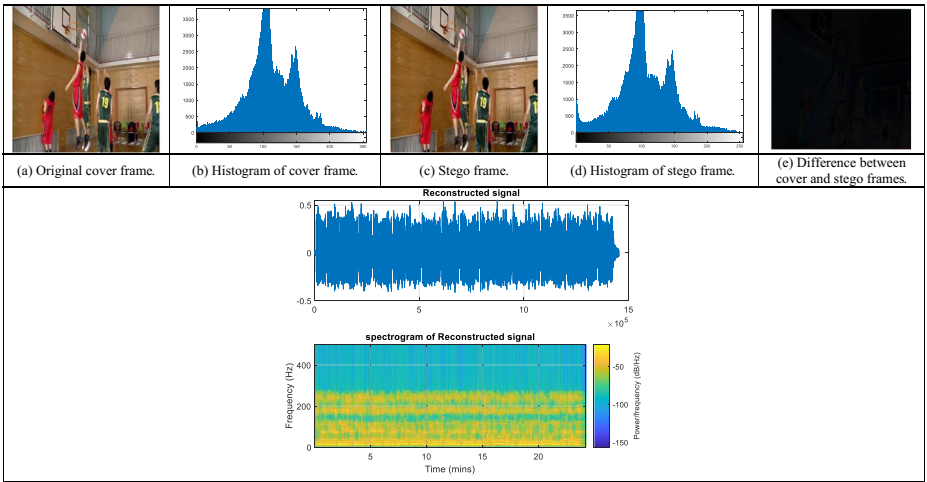


Fig. 10 The graphical results of the Balloons stream with the values of $PSNR = 31.41$ dB, $r_{xy} = 0.9974$, $SSIM = 0.9515$, $FSIM = 0.9889$, and processing time = 2.4 s in the case of using the short audio signal as a secret message



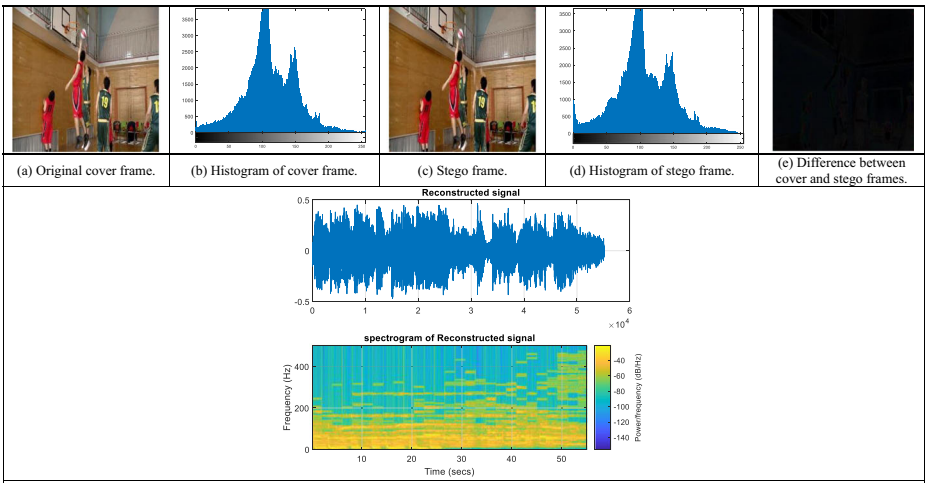
(a) Original cover frame. (b) Histogram of cover frame. (c) Stego frame. (d) Histogram of stego frame. (e) Difference between cover and stego frames.

(f) Extracted and reconstructed long audio signal and its spectrogram with the values of *SNR*=16.46dB, *SD*=2.85dB, SNR_{seg}=16.39dB, LLR=0.36dB, PRD=0.15dB, PESQ=4.23, NPCR=95.47%, UACI=28.63%, and r_{xy}=0.99.

Fig. 11 The graphical results of the Basketball stream with the values of *PSNR*=34.80dB, *rxy*=0.9949, *SSIM*=0.9476, *FSIM*=0.9882, and processing time=3.7 sec in the case of using the long audio signal as a secret message

$$SSIM = \frac{\left(2\mu_x\mu_y + V_1\right)\left(2\sigma_x + V_2\right)}{\left(\mu_x^2 + \mu_y^2 + V_1\right)\left(\sigma_x^2 + \sigma_y^2 + V_2\right)} \tag{37}$$

where σ_x and μ_x denote to the standard deviation and the mean values of pixels in an original frame x, respectively. The σ_y and μ_y denote to the standard deviation and the



(a) Original cover frame. (b) Histogram of cover frame. (c) Stego frame. (d) Histogram of stego frame. (e) Difference between cover and stego frames.

(f) Extracted and reconstructed short audio signal and its spectrogram with the values of *SNR*=14.99dB, *SD*=3.48dB, SNR_{seg}=14.88dB, LLR=0.32dB, PRD=0.11dB, PESQ=3.95, NPCR=96.58%, UACI=29.31%, and r_{xy}=0.98.

Fig. 12 The graphical results of the Basketball stream with the values of $PSNR = 34.92$ dB, $r_{xy} = 0.9956$, $SSIM = 0.9477$, $FSIM = 0.9890$, and processing time = 2.45 s in the case of using the short audio signal as a secret message

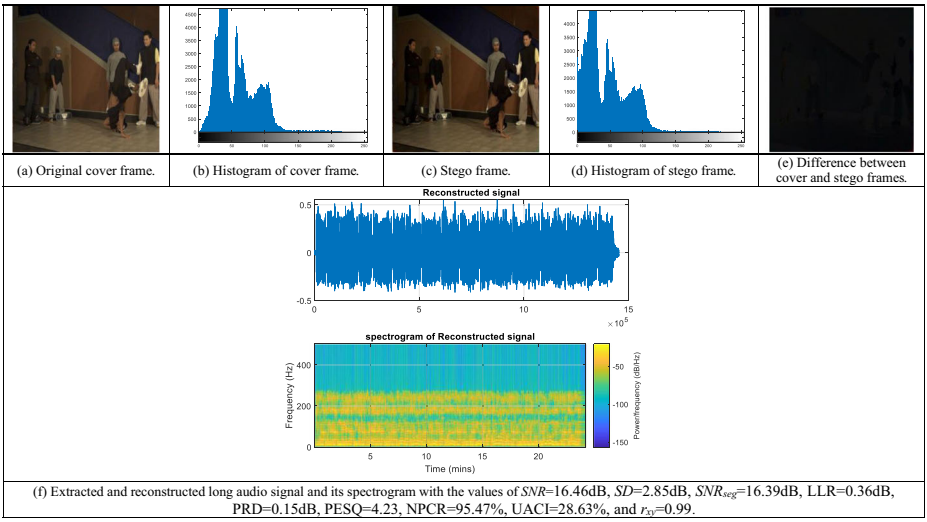


Fig. 13 The graphical results of the Breakdancer stream with the values of $PSNR = 32.04$ dB, $r_{xy} = 0.9957$, $SSIM = 0.9359$, $FSIM = 0.9844$, and processing time = 3.4 s in the case of using the long audio signal as a secret message

mean values of pixels in a stego frame y, respectively. The V_1 and V_2 are constants with small values.

The $FSIM$ is also calculated for evaluating the quality and efficiency of the proposed approach. It determines the amount of local similarity amongst the original frame and stego frame as follows:

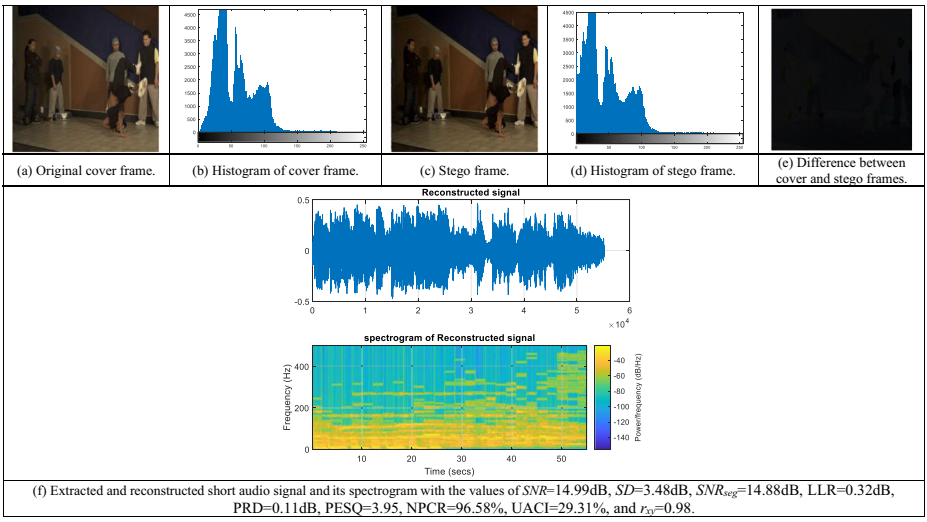
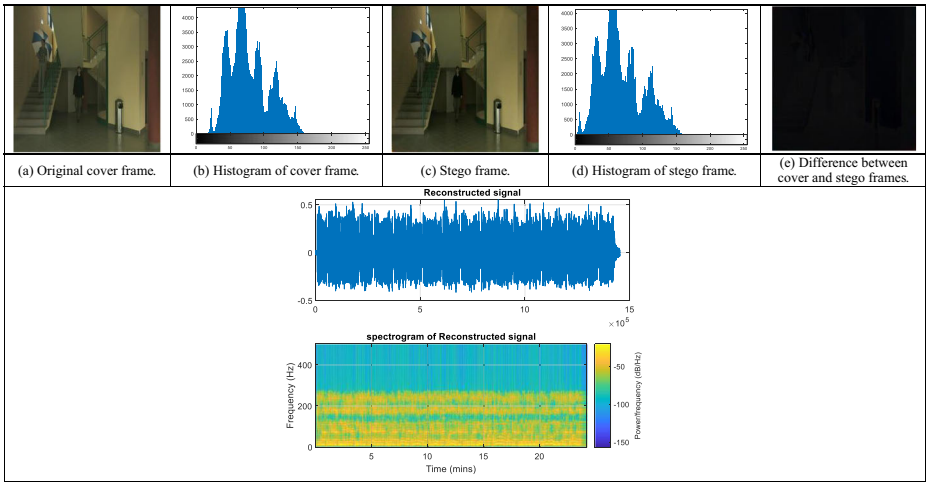


Fig. 14 The graphical results of the Breakdancer stream with the values of $PSNR = 32.07$ dB, $r_{xy} = 0.9968$, $SSIM = 0.9358$, $FSIM = 0.9863$, and processing time = 2.28 s in the case of using the short audio signal as a secret message

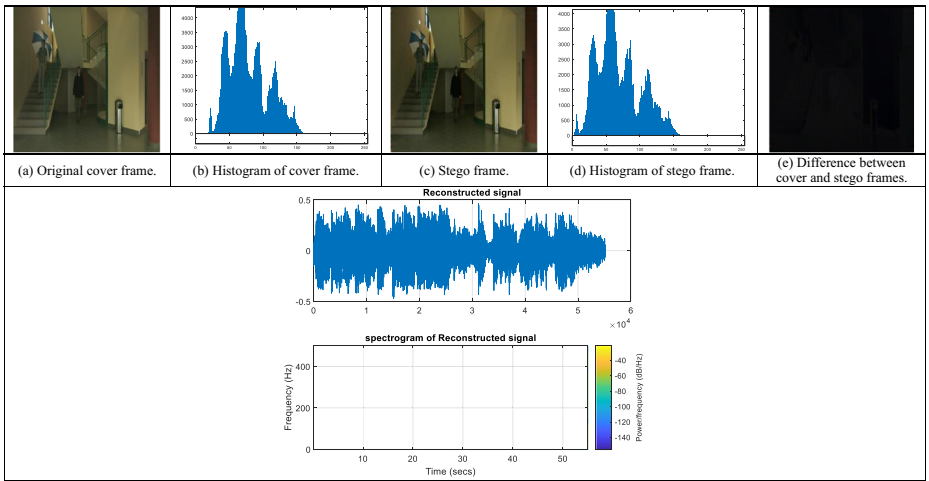


(f) Extracted and reconstructed long audio signal and its spectrogram with the values of *SNR*=16.46dB, *SD*=2.85dB, SNR_{seg}=16.39dB, LLR=0.36dB, PRD=0.15dB, PESQ=4.23, NPCR=95.47%, UACI=28.63%, and r_{xy}=0.99.

Fig. 15 The graphical results of the PoznanHall stream with the values of $PSNR = 31.32$ dB, $r_{xy} = 0.9960$, $SSIM = 0.9199$, $FSIM = 0.9890$, and processing time = 3.8 s in the case of using the long audio signal as a secret message

$$FSIM = \frac{\sum_{x \in \Omega} S_L(x).PC_m(x)}{\sum_{x \in \Omega} PC_m(x)} \tag{38}$$

where the $PC_m(x)$ is the estimated value of the phase congruency, Ω is the spatial domain of the video frame, and the $S_L(x)$ is the overall estimated similarity amongst the two frames. For improved steganography quality, it is desired to have a higher *FSIM* value for the stego frame (the value of the *FSIM* metric increases when the steganography efficiency is increased).



(f) Extracted and reconstructed short audio signal and its spectrogram with the values of *SNR*=14.99dB, *SD*=3.48dB, SNR_{seg}=14.88dB, LLR=0.32dB, PRD=0.11dB, PESQ=3.95, NPCR=96.58%, UACI=29.31%, and r_{xy}=0.98.

Fig. 16 The graphical results of the PoznanHall stream with the values of $PSNR = 31.42$ dB, $r_{xy} = 0.9973$, $SSIM = 0.9203$, $FSIM = 0.9905$, and processing time = 2.73 s in the case of using the short audio signal as a secret message

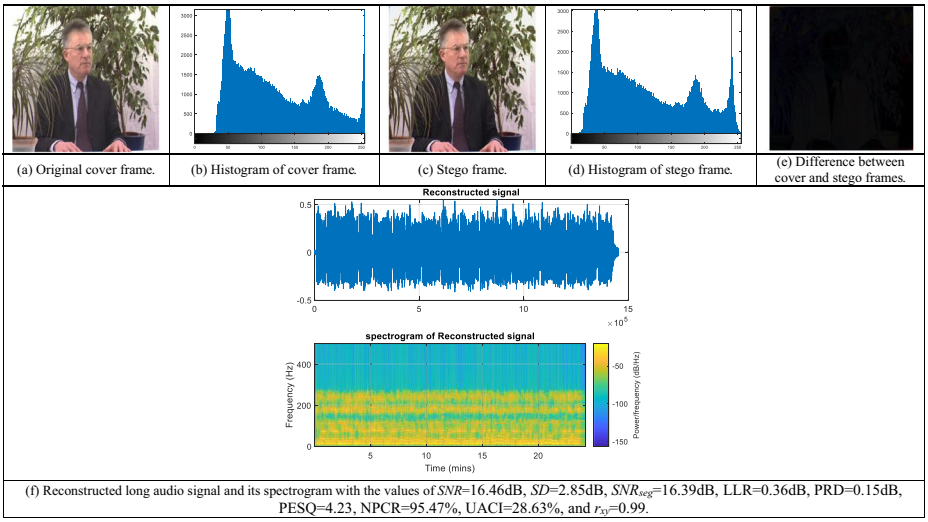


Fig. 17 The graphical results of the Uli stream with the values of $PSNR = 35.85$ dB, $r_{xy} = 0.9961$, $SSIM = 0.9477$, $FSIM = 0.9875$, and processing time = 3.58 s in the case of using the long audio signal as a secret message

To further validate the effective performance of the proposed steganography approach, the correlation coefficient (r_{xy}) amongst the stego and the original frames is also measured that assess the quality of the proposed approach. It can be calculated as defined in Eq. (35), where in this case the $c_v(x, y)$ is the covariance value amongst the processed stego and original video frames, respectively, while the $D(y)$ and $D(x)$ determine the values of the variances of the two frames y and x, respectively. To achieve a better quality of the proposed steganography process, the *PSNR*, *SSIM*, *FSIM*, and r_{xy} should record higher values amongst the processed stego and original HEVC frames.

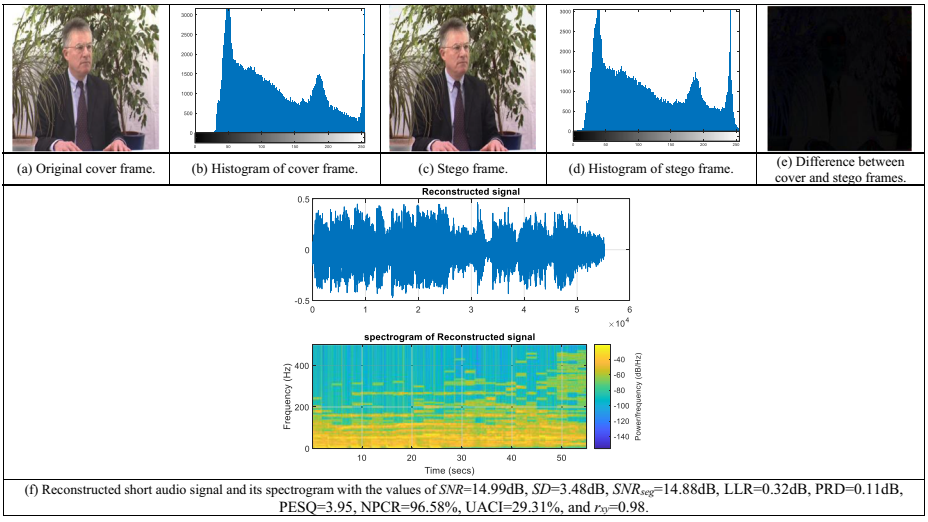


Fig. 18 The graphical results of the balloons stream with the values of $PSNR = 35.94$ dB, $r_{xy} = 0.9966$, $SSIM = 0.9478$, $FSIM = 0.9885$, and processing time = 2.84 s in the case of using the short audio signal as a secret message

Table 2 The results of quality metrics of the extracted and reconstructed long and short audio signals in the occurrence of various rotation attacks on the stego HEVC frames

Quality metric	Long signal			Short signal		
	Rotation 10°	Rotation 20°	Rotation 30°	Rotation 10°	Rotation 20°	Rotation 30°
SNR (dB)	16.21	16.04	15.86	14.76	14.53	14.37
SD (dB)	2.98	3.12	3.29	3.64	3.79	3.94
SNR_{seg} (dB)	16.17	15.96	15.74	14.62	14.49	14.22
LLR (dB)	0.35	0.33	0.32	0.30	0.29	0.27
PRD (%)	0.142	0.127	0.104	0.102	0.092	0.071
PESQ	4.21	4.18	4.15	3.92	3.90	3.87
NPCR (%)	95.48	95.39	95.55	96.61	96.49	96.63
UACI (%)	28.66	28.59	28.76	29.42	29.51	29.49
r_{xy}	0.96	0.91	0.87	0.95	0.89	0.82

In the simulation results, different values for γ and α percentages have been utilized for evaluating both the extracted and embedded secret data. Moreover, the cover HEVC frame is matched to the stego one to decide if there is a noticeable difference between them or not. The amount of indication difference can be studied as a relationship evaluation metric, and it can regulate the high limit of the embedding information capacity. To provide the carrier to be secured, and the hidden message involved in it cannot be discovered by the known statistical analysis methods, the length of this secret message should be less than the predefined upper bound. It has been found that when $\alpha = 15$ and $\gamma = 95$, we obtain a very good quality of both audio and video frames.

Figures 9, 10, 11, 12, 13, 14, 15, 16, 17 and 18 present the graphical results of the proposed steganography process that are performed to hide an audio secret message within the tested five different HEVC streams in the two cases of using long and short audio signals as secret messages. Each one of these figures shows the results of the original and stego frames of the utilized HEVC stream and their histograms, it also introduces the difference amongst the stego and cover frames, and the extracted and reconstructed secret audio signal. Also, each one of these figures presents the objective results of the *PSNR*, *SSIM*, *FSIM*, r_{xy}, and processing time of the stego frames, also it presents the objective results of the *SNR*, SNR_{seg}, *SD*, LLR, PRD, PESQ, NPCR, UACI, and r_{xy} of the reconstructed secret audio signal. Figs. 9, 11, 13, 15, and

Table 3 The results of quality metrics of the extracted and reconstructed long and short audio signals in the occurrence of various Gaussian noise attacks on the stego HEVC frames

Quality metric	Long signal			Short signal		
	Gaussian noise 0.01	Gaussian noise 0.05	Gaussian noise 0.1	Gaussian noise 0.01	Gaussian noise 0.05	Gaussian noise 0.1
SNR (dB)	16.40	16.35	16.27	14.84	14.79	14.71
SD (dB)	2.91	2.98	3.08	3.62	3.76	3.87
SNR_{seg} (dB)	16.32	16.28	16.19	14.82	14.76	14.68
LLR (dB)	0.35	0.33	0.30	0.31	0.28	0.26
PRD (%)	0.149	0.126	0.108	0.115	0.097	0.073
PESQ	4.22	4.17	4.13	3.93	3.89	3.84
NPCR (%)	95.52	95.48	95.67	96.59	96.62	96.72
UACI (%)	28.79	28.72	28.67	29.52	29.57	29.53
r_{xy}	0.97	0.95	0.91	0.97	0.92	0.89

Table 4 The results of quality metrics of the extracted and reconstructed long and short audio signals in the occurrence of various blurring attacks on the stego HEVC frames

Quality metric	Long signal			Short signal		
	Motion blur	Average blur	Disk blur	Motion blur	Average blur	Disk blur
SNR (dB)	16.29	16.33	16.13	14.76	14.81	14.53
SD (dB)	3.15	2.91	3.27	3.82	3.58	3.97
SNR_{seg} (dB)	16.18	16.31	16.05	14.64	14.72	14.38
LLR (dB)	0.33	0.34	0.32	0.29	0.31	0. 27
PRD (%)	0.132	0.145	0.121	0.094	0.107	0.109
PESQ	4.18	4.21	4.16	3.89	3.92	3.87
NPCR (%)	95.56	95.68	95.52	96.62	96.74	96.68
UACI (%)	28.69	28.83	28.72	29.64	29.59	29.81
r_{xy}	0.93	0.95	0.87	0.92	0.94	0.86

17 show the results of the employed HEVC frames in the case of using the long audio signal as a secret message, while Figs. 10, 12, 14, 16, and 18 show the results of the employed HEVC frames in the case of using the short audio signal as a secret message.

As it is known that the three basic requirements of video steganography process are the capacity, robustness, and imperceptibility. To achieve a good imperceptibility which is the most essential need for the video steganography process, the transmitted video should have high quality without causing anyone to discover it. To ensure the ability of the proposed HEVC steganography approach for achieving high imperceptibility, several HEVC streams with different dimensions have been used in the simulation tests, to embed long and short audio messages utilizing the maximum capacity of the video frames. All results presented in Figs. 9, 10, 11, 12, 13, 14, 15, 16, 17 and 18 demonstrate the performance efficacy of the suggested steganography performance in capacity, robustness, and imperceptibility perspectives.

It is observed from all introduced results that the stego frames are approximately similar to the original cover frames, so this proves higher imperceptibility performance of the proposed steganography approach. Also, it is noticed that there is a great possibility to hide a long or short audio secret message within the HEVC frames with achieving higher quality, so this proves the higher capacity accomplishment of the suggested steganography scheme.

Table 5 The results of quality metrics of the extracted and reconstructed long and short audio signals in the occurrence of various JPEG compression attacks on the stego HEVC frames

Quality metric	Long signal			Short signal		
	JPEG 10%	JPEG 20%	JPEG 30%	JPEG 10%	JPEG 20%	JPEG 30%
SNR (dB)	16.30	16.35	16.41	14.79	14.87	14.93
SD (dB)	3.07	2.93	2.89	3.75	3.67	3.54
SNR_{seg} (dB)	16.12	16.24	16.36	14.64	14.38	14.72
LLR (dB)	0.32	0.34	0.35	0.28	0.30	0.31
PRD (%)	0.141	0.146	0.149	0.104	0.106	0.109
PESQ	4.17	4.19	4.22	3.89	3.91	3.94
NPCR (%)	95.54	95.51	95.48	96.49	96.52	96.56
UACI (%)	28.52	28.57	28.61	29.18	29.23	29.29
r_{xy}	0.88	0.93	0.96	0.89	0.92	0.96

Table 6 The results of quality metrics of the extracted and reconstructed long and short audio signals in the occurrence of crop and resizing attacks on the stego HEVC frames

Quality metric	Long signal		Short signal	
	Crop attack	Resize attack	Crop attack	Resize attack
SNR (dB)	15.82	16.31	14.14	14.71
SD (dB)	3.69	3.13	3.78	3.67
SNR_{seg} (dB)	15.79	16.12	14.67	14.51
LLR (dB)	0.32	0.35	0.28	0.30
PRD (%)	0.124	0.142	0.096	0.107
PESQ	4.17	4.19	3.88	3.92
NPCR (%)	95.52	95.67	96.68	96.73
UACI (%)	28.69	28.71	29.42	29.51
r_{xy}	0.86	0.91	0.85	0.93

Furthermore, it is also demonstrated from the results shown in Figs. 9, 10, 11, 12, 13, 14, 15, 16, 17 and 18 that there is a possibility to extract and reconstruct the secret audio signal with higher quality, so this proves the higher robustness performance of the proposed steganography approach. Therefore, the proposed QFFT-based HEVC steganography approach has a high level of imperceptibility, while the PSNR measurements with a good performance above 20 dB for the whole analyzed HEVC frames in case of various lengths of audio secret messages. Moreover, it achieves higher SSIM, FSIM, and r_{xy} values. Besides, it is noticed that the suggested approach has a superior level of robustness since the original audio message is recovered with higher PESQ, SNR, SNRseg, and r_{xy} values with achieving lower LLR, PRD, NPCR, UACI, and SD values.

To further evaluate the efficiency of the proposed QFFT-based HEVC steganography approach, we tested its performance in the presence of attacks. We carried out more simulation tests in the case of existing various kinds of communication attacks of the rotation, Gaussian noise, blurring, JPEG compression, resizing, and crop attacks. Tables 2, 3, 4, 5 and 6 present the objective *SNR*, SNR_{seg}, SD, LLR, PRD, PESQ, NPCR, UACI, and r_{xy} values of the extracted and reconstructed secret long and short audio signals for the proposed steganography approach at various kinds of channel attacks. It is observed from the whole investigated results in Tables 2, 3, 4, 5 and 6 that the suggested QFFT-based HEVC steganography approach has a high level of robustness since the original secret long and short audio messages can be extracted and reconstructed with good quality metrics of the *SNR*, SNR_{seg}, *SD*, LLR, PRD, PESQ, NPCR, UACI, and r_{xy} values.

Furthermore, the proposed QFFT-based HEVC steganography scheme is contrasted to some recent literature HEVC steganography works to prove its superior performance

Table 7 The PSNR and SSIM comparison outcomes of the suggested steganography algorithm and the literature algorithms in [5, 7, 22, 27]

Steganography scheme	PSNR (dB)	SSIM
Proposed	34.93	0.95
Ref. [27]	33.15	0.92
Ref. [5]	34.27	0.94
Ref. [22]	34.54	0.92
Ref. [7]	33.81	0.94

efficiency. Table 7 introduces the SSIM and PSNR comparison objective outcomes for the HEVC Basketball stream of the proposed HEVC steganography algorithm and the literature HEVC steganography algorithms in [5, 7, 22, 27]. It is observed that the proposed steganography approach presents higher PSNR and SSIM values compared to the literature approaches for the tested Basketball stream which proves its great imperceptibility and efficiency.

5 Conclusions and future work

This article introduced a new QFFT-based HEVC steganography approach. The proposed approach could be applied for embedding secret audio messages in cover video frames. Thus, in this paper, secret audio data has been concealed inside HEVC cover frames. The audio message is firstly compressed to exploit the capacity of cover video frames, and consequently maximizing the size of the hidden message as possible. Furthermore, the compressed secret message is then encrypted using a random projection encryption method in the DWT domain. The random matrix of the random projection of the compressed message is generated using the Legendre sequence to produce the encrypted form of the compressed secret data. The compressed HEVC cover frames and secret data are assigned to the quaternion format in the QFFT domain prior to the hiding process. The proposed approach has been tested through various standard HEVC streams and audio signals. The accomplishment of the suggested approach is evaluated by assessing different quality metrics with and without the presence of different multimedia attacks. The achieved outcomes proved that the cover video frames can be communicated with no obvious variation with a high imperceptibility compared to the literature algorithms. Furthermore, the obtained findings clarified the chance of inserting secret data with large size with achieving higher embedding capacity and exploiting the whole size of the cover video frame. In this paper, we did not utilize watermarking besides employed encryption and steganography schemes. So, in the future, we can enhance the performance of the HEVC steganography approach by integrating the watermarking process in addition to the presented work to build a multi-level security system for HEVC transmission and storage. Also, new trends of deep learning-based security approaches can be utilized for HEVC transmission and storage to achieve covert and robust performance.

Acknowledgements This research was funded by the Dean of Scientific Research at princess Nourah bint Abdulrahman University. Grant No. (39/S/250). And the authors would like to thank this support.

References

1. Alyousuf FQA, Din R, Qasim AJ (2020) Analysis review on spatial and transform domain technique in digital steganography. Bulletin of Electrical Engineering and Informatics 9(2):573–581
2. Bahrami Z, Tab FA (2018) A new robust video watermarking algorithm based on SURF features and block classification. Multimed Tools Appl 77(1):327–345
3. Balu S, Babu CNK, Amudha K (2019) Secure and efficient data transmission by video steganography in medical imaging system. Clust Comput 22(2):4057–4063
4. Dasgupta K, Mondal JK, Dutta P (2013) Optimized video steganography using genetic algorithm (GA). Procedia Technology 10:131–137

5. Dong, Y, Sun, T and Jiang, X (2018). A high capacity HEVC Steganographic algorithm using intra prediction modes in multi-sized prediction blocks. In international workshop on digital watermarking (pp. 233-247). Springer, Cham
6. EL-Latif AAA, Abd-El-Atty B, Venegas-Andraca SE (2019) A novel image steganography technique based on quantum substitution boxes. Opt Laser Technol 116:92–102
7. Galiano DR, Del Barrio AA, Botella G, Cuesta D (2020) Efficient embedding and retrieval of information for high-resolution videos coded with HEVC. Comput Electr Eng 81:106541
8. Golomb, SW (1967). Shift register sequences. Aegean Park Press
9. Hamilton, WR (1844). On a new species of imaginary quantities connected with a theory of quaternions. In proceedings of the Royal Irish Academy (Vol. 2, no. 424-234, pp. 4-1)
10. Hashemzadeh M (2018) Hiding information in videos using motion clues of feature points. Comput Electr Eng 68:14–25
11. HEVC Reference software (2014). http://hevc.kw.bbc.co.uk/trac/browser/jctvc-hm/tags
12. Hitzer E (2016) The quaternion domain Fourier transform and its properties. AACA 26(3):969–984
13. Hussain M, Wahab AWA, Idris YIB, Ho AT, Jung KH (2018) Image steganography in spatial domain: A survey. Signal Process Image Commun 65:46–66
14. Hussain, I, Zeng, J and Tan, S (2020). A survey on deep convolutional neural networks for image steganography and Steganalysis. KSII Trans Internet Inf Syst, 14(3)
15. Junjie, W, Qian, M, Dongxia, M and Jun, Y (2009). Research for synchronic audio information hiding approach based on DWT domain. In 2009 international conference on E-business and information system security (pp. 1-5). IEEE
16. Kadhim IJ, Premaratne P, Vial PJ, Halloran B (2019) Comprehensive survey of image steganography: techniques, evaluations, and trends in future research. Neurocomputing 335:299–326
17. Kaur H, Khanna P (2015) Gaussian random projection based non-invertible cancelable biometric templates. Procedia Computer Science 54:661–670
18. Khalil MI (2012) Applying quaternion Fourier transforms for enhancing color images. International Journal of Image, Graphics and Signal Processing 4(2):9
19. Khalil MI (2017) Quaternion-based encryption/decryption of audio signal using digital image as a variable key. International Journal of Communication Networks and Information Security 9(2):216
20. Khalil MI (2018) Using quaternion Fourier transform in steganography systems. International Journal of Communication Networks and Information Security 10(2):425–431
21. Khosravi MR, Samadi S (2019) Reliable data aggregation in internet of ViSAR vehicles using chained dual-phase adaptive interpolation and data embedding. IEEE Internet Things J 7(4):2603–2610
22. Konyar, MZ, Akbulut, O and Öztürk, S (2020). Matrix encoding-based high-capacity and high-fidelity reversible data hiding in HEVC. Signal, Image and Video Processing, 1–9
23. Kumar M, Yadav M (2014) Image steganography using frequency domain. Int J Sci Technol Res 3(9):226–230
24. Liu Z, Chen H, Sun S (2020) Research on covert communication security based on screen content coding. IEEE Access 8:22275–22280
25. Liu Y, Liu S, Wang Y, Zhao H, Liu S (2019) Video steganography: A review. Neurocomputing 335:238–250
26. Liu ZH, Luo D, Huang JW, Wang J, Qi CD (2017) Tamper recovery algorithm for digital speech signal based on DWT and DCT. Multimed Tools Appl 76(10):12481–12504
27. Liu S, Xu D (2020) A robust steganography method for HEVC based on secret sharing. Cogn Syst Res 59: 207–220
28. Manisha S, Sharmila TS (2019) A two-level secure data hiding algorithm for video steganography. Multidim Syst Sign Process 30(2):529–542
29. Mansouri J, Khademi M (2009) An adaptive scheme for compressed video steganography using temporal and spatial features of the video signal. Int J Imaging Syst Technol 19(4):306–315
30. Mareen H, De Praeter J, Van Wallendael G, Lambert P (2018) A novel video watermarking approach based on implicit distortions. IEEE Trans Consum Electron 64(3):250–258
31. Matoušek J (2008) On variants of the Johnson–Lindenstrauss lemma. Random Struct Algoritm 33(2):142–156
32. Mihara T (2015) Quantum steganography using prior entanglement. Phys Lett A 379(12–13):952–955
33. Mstafa RJ, Elleithy KM, Abdelfattah E (2017) A robust and secure video steganography method in DWT-DCT domains based on multiple object tracking and ECC. IEEE Access 5:5354–5365
34. Müller K, Vetro A (2014) Common test conditions of 3DV core experiments. ITU-T SG 16:1–7
35. Nabil, M (2017). Random projection and its applications. arXiv preprint arXiv:1710.03163

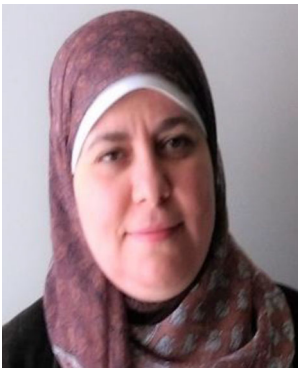
36. Noda, H, Furuta, T, Niimi, M and Kawaguchi, E (2004). Application of BPCS steganography to wavelet compressed video. In 2004 international conference on image processing, 2004. ICIP'04. (Vol. 4, pp. 2147-2150). IEEE
37. Patel VM, Ratha NK, Chellappa R (2015) Cancelable biometrics: A review. IEEE Signal Process Mag 32(5):54–65
38. Pillai JK, Patel VM, Chellappa R, Ratha NK (2011) Secure and robust iris recognition using random projections and sparse representations. IEEE Trans Pattern Anal Mach Intell 33(9):1877–1893
39. Qu Z, Cheng Z, Liu W, Wang X (2019) A novel quantum image steganography algorithm based on exploiting modification direction. Multimed Tools Appl 78(7):7981–8001
40. Rakhmawati L, Wirawan W, Suwadi S (2019) A recent survey of self-embedding fragile watermarking scheme for image authentication with recovery capability. EURASIP Journal on Image and Video Processing 2019(1):61
41. Ramalingam M, Isa NAM (2015) Fast retrieval of hidden data using enhanced hidden Markov model in video steganography. Appl Soft Comput 34:744–757
42. Rawat C, Meher S (2013) A hybrid image compression scheme using DCT and fractal image compression. Int Arab J Inf Technol 10(6):553–562
43. Sadat ES, Faez K, Saffari Pour M (2018) Entropy-based video steganalysis of motion vectors. Entropy 20(4):244
44. Sathiyamurthi, P and Ramakrishnan, S (2020). Speech encryption algorithm using FFT and 3D-Lorenz–logistic chaotic map. Multimed Tools Appl, 1–19
45. Sheela SJ, Suresh KV, Tandur D (2017) A novel audio cryptosystem using chaotic maps and DNA encoding. Journal of Computer Networks and Communications 2017:1–12
46. Soliman NF, Mostfa Z, El-Samie FEA, Abdalla MI (2017) Performance enhancement of speaker identification systems using speech encryption and cancelable features. International Journal of Speech Technology 20(4):977–1004
47. Soria-Lorente, A and Berres, S (2017). A secure steganographic algorithm based on frequency domain for the transmission of hidden information Security and Communication Networks, 2017
48. Sushmitha, MC, Suresh, HN and Manikandan, J (2017). An approach towards novel video steganography for consumer electronics. In 2017 IEEE international conference on consumer electronics-Asia (ICCE-Asia) (pp. 72-76). IEEE
49. Suterio, V, Scalassara, PR, Agulhari, CM and Durand, FR (2019). Minimization of percent root-Mean-Square difference in the generation of wavelets using genetic algorithm. In XXVI Brazilian congress on biomedical engineering (pp. 319–325). Springer, Singapore
50. Tan, D, Lu, Y, Yan, X and Wang, X (2019). A simple review of audio steganography. In 2019 IEEE 3rd information technology, networking, electronic and automation control conference (ITNEC) (pp. 1409-1413). IEEE
51. Wang Z, Bovik AC, Sheikh HR, Simoncelli EP (2004) Image quality assessment: from error visibility to structural similarity. IEEE Trans Image Process 13(4):600–612
52. Wang J, Jia X, Kang X, Shi YQ (2019) A cover selection HEVC video steganography based on intra prediction mode. IEEE Access 7:119393–119402
53. Wang Q, Lin D, Guang X (2014) On the linear complexity of Legendre sequences over F q. IEICE Trans Fundam Electron Commun Comput Sci 97(7):1627–1630
54. Xia Z, Wang X, Sun X, Wang B (2014) Steganalysis of least significant bit matching using multi-order differences. Security and Communication Networks 7(8):1283–1291

Naglaa F. Soliman received the B.Sc., M.Sc., and Ph.D. degrees from the faculty of Engineering, Zagazig University, Egypt in 1999, 2004, and 2011, respectively. She worked at faculty of computer science at PNU, KSA. since 2015 up till now. She has been a Teaching Staff Member with the Department of Electronics and Communications Engineering, Faculty of Engineering, Zagazig University, Egypt. Her current research interests include digital image processing, Information security, multimedia communications, medical image processing, optical signal processing, big data, and cloud computing.

Magdi Ibrahim Khalil El-Sharkawy Egyptian, male, Ph.D degree in Computer System Engineering. His main research interests focus on digital signal processing and information security. So far, he has published more than twenty-five papers in repute journals and proceedings of conferences in fields of information security, digital signal processing, image processing.

Abeer D. Algarni received the B.Sc. (Hons.) in Computer Science from King Saud University, Riyadh, Saudi Arabia in 2007. She received the M.Sc., and Ph.D. degrees from School of Engineering and Computer Sciences, Durham University, United Kingdom in 2010 and 2015, respectively. She worked as an assistant professor at College of Computer and Information Sciences at Princess Nourah Bent Abdulrahman University since 2008 up till now. Her current research interests include networking and communication systems, digital image processing, digital communications and cyber security.

Sahar A. El_Rahman has received her M.Sc. (2003) in an AI Technique Applied to Machine Aided Translation, and Ph.D. (2008) in Reconstruction of High-Resolution Image from a Set of Low-Resolution Images, from the Faculty of Engineering- Shoubra, Benha University, Cairo, Egypt. She is currently Assistant Professor, College of Computer and Information System, Princess Nourah Bint Abdulrahman University (Saudia Arabia). Also, she is Assistant Professor from 2008 till now at Faculty of Engineering-Shoubra, Benha University, Cairo, Egypt. Her research interests include Computer Vision, Image Processing, Information Security, Human Computer Interaction, E-Health, Big Data and Cloud Computing.



Radwa Marzouk is an assistant professor at College of Computer and Information Sciences (CCIS), Princess Nourah Bint Abdulrahman University, Riyadh, Saudi Arabia. She is also a faculty member in Department of Mathematics, Faculty of Science, Cairo University, Egypt since 2003 till now. She received the B.S. (2000), M.S. (2005) and Ph.D. (2012) in Computer Science from Cairo University. Her primary research interests are in cryptography, computer security, coding theory, digital image processing, and applied mathematics. She has published several scientific papers in national, international conferences and journals.

Walid El-Shafai was born in Alexandria, Egypt. He received the B.Sc. degree (Hons.) in Electronics and Electrical Communication Engineering from Faculty of Electronic Engineering (FEE), Menoufia University, Menouf, Egypt in 2008, M.Sc. degree from Egypt-Japan University of Science and Technology (E-JUST) in 2012, and PhD degree from the Faculty of Electronic Engineering, Menoufia University, Menouf, Egypt in 2019. He is currently working as a Lecturer and an Assistant professor 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, 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.

Affiliations

Naglaa F. Soliman[1,2] · M. I. Khalil[3] · Abeer D. Algarni[1] · Sahar Ismail[1,4] · Radwa Marzouk[1,5] · Walid El-Shafai[6]

Naglaa F. Soliman
nagla.soliman@yahoo.com

M. I. Khalil
magdi_nrc@hotmail.com

Abeer D. Algarni
a_dalqarni@pnu.edu.sa

Sahar Ismail
saismail@pnu.edu.sa

Radwa Marzouk
rmmarzouk@pnu.edu.sa

[1] Faculty of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, Riyadh, Saudi Arabia

[2] Department of Electronics and Communications, Faculty of Engineering, Zagazig University, Zagazig, Egypt

[3] Reactor Physics Dept., NRC, Atomic Energy Authority, Cairo, Egypt

[4] Electrical Engineering Department, Faculty of Engineering-Shoubra, Benha University, Cairo, Egypt

[5] Department of Mathematics, Faculty of Science, Cairo University, Giza 12613, Egypt

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