EAI Endorsed Transactions
on Industrial Networks and Intelligent Systems

Review Article/EAI.EU

LSB Data Hiding in Digital Media: A Survey

Dang Ninh Tran[1]*, Hans-Jürgen Zepernick[1], and Thi My Chinh Chu[1]

[1]Blekinge Institute of Technology, SE-371 79 Karlskrona, Sweden;
hans-jurgen.zepernick@bth.se (H.J.Z.);
thi.my.chinh.chu@bth.se (T.M.C.C.).

Abstract

Data hiding or information hiding is a prominent class of information security that aims at reliably conveying secret data embedded in a cover object over a covert channel. Digital media such as audio, image, video, and three-dimensional (3D) media can act as cover objects to carry such secret data. Digital media security has acquired tremendous significance in recent years and will be even more important with the development and delivery of new digital media over digital communication networks. In particular, least significant bit (LSB) data hiding is easy to implement and to combine with other hiding techniques, offers high embedding capacity for data, can resist steganalysis and several types of attacks, and is well suited for real-time applications. This article provides a comprehensive survey on LSB data hiding in digital media. The fundamental concepts and terminologies used in data hiding are reviewed along with a general data hiding model. The five attributes of data hiding, i.e., capacity, imperceptibility, robustness, detectability, and security, and the related performance metrics used in this survey to compare the characteristics of the different LSB data hiding methods are discussed. Given the classification of data hiding methods with respect to audio, image, video, and 3D media, a comprehensive survey of LSB data hiding for each of these four digital media is provided. In particular, landmark studies, state-of-the-art approaches, and applications of LSB data hiding are described for each of the four digital media. Their performance is compared with respect to the data hiding attributes which illustrates benefits and drawbacks of the reviewed LSB data hiding methods. The article concludes with summarizing main findings and suggesting directions for future research. This survey will be helpful for researchers and practitioners to keep abreast about the potential of LSB data hiding in digital media and to develop novel applications based on suitable performance trade-offs between data hiding attributes.

Received on 12 March 2022; accepted on 04 April 2022; published on 05 April 2022

Keywords: LSB data hiding, steganography, watermarking, audio, image, video, 3D media, performance assessment

doi:10.4108/eai.5-4-2022.173783

1. Introduction

The advancements in digital communication systems have paved the way for the widespread use of digital media over networks. The digital media types range from conventional audio, image, and video to the more recently appearing networked immersive or three-dimensional (3D) media such as 360° videos, virtual reality (VR), and augmented reality (AR). Because digital media are exchanged over wired and wireless networks, a major concern is to ensure the privacy, integrity, and security of the media data exchanged among individuals, companies, institutions, agencies, and governments. Subject to the sizes of digital media files, these resources can also be used to hide a suitable amount of secret data in these files such that it is concealed during transmission.

In recent years, information security has therefore become an integral part of digital media communication systems providing data confidentiality, data integrity, user authentication, and non-repudiation. The aims of information security include preventing access from adversaries to secret information and hiding the existence of secret information. These aims can be achieved through cryptography and information hiding. Cryptography focuses on securely protecting the

*Corresponding author: Dang Ninh Tran;
Tel.: +46-703-302-78-78.
Email: dang.ninh.tran@bth.se

content of secret messages to prevent unauthorized access to information by converting the secret information (plaintext) into an unintelligible format (ciphertext) using a suitable cipher (key). On the other hand, information hiding, also referred to as data hiding, provides covert communication between two parties hiding the very existence of the data such that the information exchange cannot be observed by an attacker. In general terms, a secret object is embedded into a cover object to constitute a stego-object. Watermarking may be regarded as a special case of data hiding where a digital watermark is hidden in the cover object to support identifying ownership and copyright. Because the human auditory system (HAS) and human visual system (HVS) are both relatively insensitive to small changes in digital media, hiding secret data in digital audio, image, video, and 3D media has been increasingly used.

In view of running data hiding algorithms on, e.g., Internet of Things (IoT) devices or mobile devices, it is desirable to engage light-weight data hiding techniques in order to minimize latency and power consumption both incurred due to processing complexity. For example, immersive media services are delay sensitive with motion-to-photon latency to be kept below 20 ms. Data hiding must be executed within this delay budget while keeping computational load low. Least significant bit (LSB) data hiding may therefore be considered as it is easy to implement and to combine with other hiding techniques, offers high embedding capacity for data, can resist steganalysis and several types of attacks, and is well suited for real-time applications. Furthermore, as only LSBs or potentially some higher bit planes of the cover digital media are modified, the hidden data is more or less imperceptible by the HAS or HVS. While surveys on data hiding in digital media focus on either audio, image, video, or 3D media but cover a wide range of data hiding approaches, this survey is dedicated to LSB data hiding but covers the mentioned wide range of digital media.

In the following sections of this introduction, fundamentals of data hiding, attributes and performance metrics of data hiding techniques, a discussion of surveys on data hiding in digital media, and a classification of LSB data hiding techniques are provided leading to the motivation and contributions of the work reported in this paper. The rest of this survey is then organized as follows. Section 2 provides the survey of LSB data hiding in digital audio including speech and voice with respect to the temporal, transform, and coded domains. Section 3 contains the LSB data hiding techniques used with digital images considering the spatial, transform, and quantum domains. A survey on LSB data hiding in raw and compressed data formats of digital videos is provided in Section 4. Section 5 focuses on LSB data hiding in 3D media, i.e., 3D mesh media, 3D anaglyph media, and 360° media. Finally, Section 6 provides a summary of the survey, presents main findings, and suggests some directions for future research.

1.1. Fundamentals of Data Hiding

Cryptography and information hiding (or data hiding) [1] are the two main approaches for secure communication in the presence of a malicious entity called adversary [2]. These malicious third parties attempt, e.g., to discover or corrupt the secret data, and to spoof the identity of the legitimate users among many other potential malicious attacks.

Cryptography. This information security approach focuses on protecting secret data using encryption which transforms plaintext into ciphertext. Typically, a pseudo-random encryption key is used with an encryption scheme to transform secret data into a noise-like data stream. Objectives of cryptography include securing the confidentiality of the secret data, data integrity in terms of accuracy and consistency, authentication of legitimate users, and non-repudiation such as proofing integrity and origin of data as well as genuine authentication with high confidence.

Information hiding. This approach is concerned with providing methods that hide the very existence of secret data such that it does not attract suspicion by an adversary [3]. Information hiding includes copyright and ownership protection of digital media using watermarking, authentication based on fingerprinting, and communicating secret data using a suitable carrier.

Steganography is a prominent class of information hiding that aims at reliably conveying secret data embedded in a cover object over a covert channel. Specifically, a secret object is hidden in an appropriate cover object such that it is imperceptible to an adversary in the resulting stego-object. Since the HAS and HVS are relatively insensitive to small changes in digital media, hiding secret information in digital audio, images, and videos has increasingly been used. A benefit of steganography over cryptography is that it may arouse less suspicion. Many digital media steganography methods have been proposed for conventional digital audio, image, and video formats that act as cover object for secret data. Steganography for new digital media is less developed due to immersive digital media themselves being still in the process of further development. In summary, the goal of steganography is achieved if the communication channel is covert and the secret information being any type of data is not detected.

Watermarking focuses on authentication of the communication and the data transferred. The secret object has a close relationship with the cover object which can be the information about the owner,

copyright, or special characteristics of the cover object. The secret object carried in the stego-object can be perceptible or imperceptible depending on the watermark design. Overall, the goal of watermarking is achieved if copyright protection exists and the watermark is not erased or tampered.

Data hiding. Information hiding and data hiding have been used interchangeably [1]. In [4], referring to [5], data hiding is recalled being the process of hiding data that represents some information into cover media. In other words, the data hiding process links a set of secret or embedded data with a set of cover media data. The relationship between these two sets of data depends on the aim of the applications, e.g., steganography or watermarking. Because this survey focuses on hiding data in digital media, we will mainly use the term data hiding. The most popular model of data hiding was proposed at the first workshop on information hiding in 1996 [6] which may be applied to steganography and watermarking. Related terminologies used in this context are explained in the following with reference to Fig. 1.

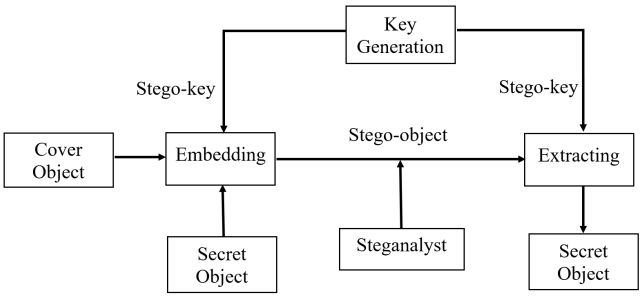

Figure 1. Data hiding model (see also [6]).

- **A secret object** is something, e.g., audio, image, video, or 3D media file, that shall be embedded into another object. Because digital media are presented in binary form as bitstream, the term "secret bits" is sometimes used.
- **A stego-object** is the output of the hiding process, i.e., an object that is modified to cover or conceal the secret object. The stego-object is transferred transparently and its content is monitored during the transmission. A stego-object is called watermarked object in case data hiding is used for the purpose of watermarking.
- **A cover object** is the original version of the stego-object before being modified.
- **A stego-key** is a piece of additional information needed to control the hiding process. For example, key generation in wireless network security can be found in [7, 8].
- **Embedding** is the process of hiding the secret object into the cover object.
- **Extracting** is the process of retrieving the secret object from the stego-object.
- **A steganalyst** is the entity trying to detect the secret object that is embedded in the stego-object. Depending on the aims, a steganalyst can extract, modify, remove the secret object, or even corrupt the transmission.

LSB data hiding. LSB data hiding is a method that uses LSB insertion or manipulation to embed secret bits into a cover object. The rationale behind LSB data hiding in relation to applications in digital media is that the LSBs carry only minor information and small modifications in these bits are imperceptible to the HAS and HVS. Given the increasing data volumes associated with digital media, e.g., high-definition images and videos, large capacity for data hiding is obtained. LSB data hiding is the easiest and simplest method of data hiding in digital media which resists human attacks as minor quality degradation cannot be detected. However, the noise generated by LSB data hiding provides an opening for modern steganalysis to break such approaches using statistical analysis. As a consequence, in order to resist sophisticated steganalysis, research has been directed toward developing robust LSB data hiding techniques that combine steganography with cryptography.

1.2. Attributes of Data Hiding Techniques

Assessment of data hiding depends on the features of the algorithms themselves and the other factors such as the aim, implementation, and hiding environment [1, 9–17]. In [1, 9, 14], nearly a dozen of attributes are considered for characterizing data hiding techniques. The most popular attributes of data hiding techniques are capacity, imperceptibility, robustness, detectability, and security which are described in the following along with related performance metrics.

Capacity. Payload capacity, embedding capacity, or hiding capacity, also referred as capacity for brevity, refers to the number of secret bits that can be embedded in a cover object. Different types of cover objects may use different definitions of capacity.

For audio, capacity is the hiding rate measuring the number of secret bits transferred in each second or bits per second (bps). Other measures of capacity that are used in the temporal domain of audio signals include bits per sample (bits/sample), bits per byte (bits/byte), and quantum bits (qubits) per sample (qubits/sample). Further, bits per selected coefficient (bits/sc) is used in the transform domain while bits per frame (bits/frame) with reference to the frame structure of the audio encoding format is often used in the coded domain.

For digital images, capacity is measured in terms of the average number of bits hidden in a pixel of the cover image or bits per pixel (bpp). In the transform domain, bits per coefficient (bpc) is often used as a measure of capacity.

For digital videos, capacity can be defined as the average number of secret bits concealed in each video frame and is given in bits per pixel per frame (bpp/frame). Alternative measures of capacity in the raw domain are the embedding ratio and hiding ratio. In the compressed domain of digital videos, measures of capacity include bits per non-zero coefficient (bpnzc), bits per intra-prediction mode (IPM), bits per candidate motion vector (bpcmv), and bits per label bit-carrying variable length coding (lc-VLC).

For 3D media, capacity can also be measured in bpp and bpp/frame in case 3D media are created from 2D components such as anaglyph 3D media, 360° images, and 360° videos, respectively. In case of 3D mesh models, capacity can be measured by the number of hidden bits per vertex (bpv) or number of hidden bits per coordinate (bits/coordinate), i.e., x, y, and z coordinates.

Imperceptibility. Imperceptibility refers to the ability of distinguishing between a cover object and a stego-object, which can be assessed by humans and computer analysis. A human uses the HAS and HVS to compare the differences between two objects, to assess their qualities, or to detect the distortion of the stego-object compared to the cover object. Imperceptibility is measured as degradation that is caused by the modification to the cover object. Performance measures that quantify degradation include fidelity metrics, objective quality metrics, and subjective quality assessment. Prominent measures that are used in the tabulated performance comparisons of LSB data hiding techniques in the subsequent sections are described in the following.

Signal-to-Noise Ratio (SNR): The SNR is a fidelity metric that is defined as the ratio of the signal power to the noise power and is typically measured in decibels (dB). Given a signal that is sampled in discrete time n, the SNR can be formulated as

$$\mathrm{SNR} = 10\log_{10}\left\{\frac{\sum_{n=0}^{N-1} x^2(n)}{\sum_{n=0}^{N-1}[x(n)-y(n)]^2}\right\} \tag{1}$$

where $x(n)$ represents a sample of the cover object, $y(n)$ denotes the corresponding stego-object, and N is the number of samples. In audio, the scale-invariant SNR (SI-SNR) [18] may be used which reduces the impact of volume on the evaluation results. In watermarking, the terms signal-to-watermark ratio and watermark-to-noise ratio are sometimes used depending on whether the watermark or the cover object is considered as noise. Similarly, geometrical distortion of a mesh model may be measured using the 3D signal-to-noise ratio (3D SNR).

Peak Signal-to-Noise Ratio (PSNR): The PSNR is defined as the ratio between the maximum possible power of a signal and the power of the noise that affects the fidelity of the signal's representation. For example, in the context of data hiding in videos, the mean squared error (MSE) used in the calculation of the PSNR is defined as [19]

$$\mathrm{MSE} = \frac{1}{TMN}\sum_{t=0}^{T-1}\sum_{m=0}^{M-1}\sum_{n=0}^{N-1}[I(t,m,n)-J(t,m,n)]^2 \tag{2}$$

where T denotes the number of frames of a video with given duration, M and N are the vertical and horizontal dimensions of the t-th cover frame $I(t)$ and t-th stego-frame (or watermarked frame) $J(t)$, respectively. Further, $I(t,m,n)$ and $J(t,m,n)$ are the pixels of the m-th row and n-th column of these video frames. Using (2), the PSNR is defined as

$$\mathrm{PSNR} = 10\log_{10}\frac{C_F^2}{\mathrm{MSE}} \tag{3}$$

where $C_F = 2^B - 1$ denotes the maximum value that a pixel of a video frame can take for a given bit depth B.

Structural Similarity (SSIM) Index: The SSIM index [20] is an objective metric that predicts the perceptual quality of images or videos. It evaluates image or video degradation through changes in structural information and therefore aligns with mechanisms of the HVS. Given two images or video frames I and J, the SSIM index is defined as [20]

$$SSIM(I,J) = \frac{(2\mu_I\mu_J + C_1)(2\sigma_{IJ} + C_1)}{(\mu_I^2 + \mu_J^2 + C_1)(\sigma_I^2 + \sigma_J^2 + C_2)} \tag{4}$$

where μ_I, μ_J denote the mean intensities and σ_I, σ_J are the contrasts of images I and J, respectively. Further, σ_{IJ} is the covariance between I and J, and constants C_1 and C_2 are used to stabilize the division with weak denominator.

Mean Opinions Score (MOS) [21]: Mean opinion scores are obtained from the opinion scores given during a subjective test by participants to test stimuli such as original and processed digital audio, image, video, and 3D media. The opinion scores are selected from a predefined scale, e.g., using a five-level quality scale

- 5 = excellent
- 4 = good
- 3 = fair
- 2 = poor
- 1 = bad

or a five-level impairment scale

- 5 = imperceptible
- 4 = perceptible but not annoying
- 3 = slightly annoying
- 2 = annoying
- 1 = very annoying

Here, the MOS obtained from subjective tests may relate to the cover object, stego-object, or watermarked object. As such, MOS represents a subjective measure of quality or degradation as perceived by humans.

Perceptual Evaluation of Speech Quality (PESQ) [22]: Based on a psycho-acoustic and cognitive model, the PESQ algorithm has been designed to predict subjective opinion scores of degraded speech stimuli. The quality scores predicted by PESQ range from −0.5 (worst) up to 4.5 (best) because the algorithm is optimized to estimate the average result of all listeners of a listening test. In order to allow a linear comparison with MOS, a mapping function is used on the raw scores to obtain MOS listening objective scores (MOS-LOS) scores.

Objective Difference Grade (ODG) [23]: This measure evaluates sound quality using the perceptual evaluation of audio quality (PEAQ) algorithm which assigns a comparative ODG score between 0 (indicating imperceptible impairments) and −4 (very annoying impairments). However, an ODG score might be higher than 0 as an artificial neural network is used for calculating the score. The ODG can be applied to assess the inaudibility of the modification of the original signal by the stego-signal or watermarked signal.

Spectral Distortion (SD) [24]: The SD is a measure that is calculated in the transform domain on cover-audio frequency spectra and stego-, watermarked-, or cipher-audio frequency spectra. The SD indicates how far away the stego-, watermarked-, or cipher-audio spectrum is from that of the cover-audio.

Correlation Coefficient: A correlation coefficient (CORR) quantifies the strength of the linear relationship between two variables or signals in a correlation analysis assuming values in the range from −1 to +1. The highest agreement between two variables or signals is indicated by CORR = ±1 while the highest disagreement is indicated by CORR = 0. In particular, the squared Pearson correlation coefficient (SPCC) measures the similarity between a sampled input signal x_n, $n = 0, \ldots, N-1$ (cover signal) and a sampled output signal y_n, $n = 0, \ldots, N-1$ (stego-signal or watermarked signal):

$$\mathrm{SPCC} = \left[\frac{\sum_{n=0}^{N-1} (x_n - \bar{x})(y_n - \bar{y})}{\sqrt{\sum_{n=0}^{N-1} (x_n - \bar{x})^2} \sqrt{\sum_{n=0}^{N-1} (y_n - \bar{y})^2}} \right]^2 \tag{5}$$

where $\bar{x}$ and $\bar{y}$ denote the average input signal and output signal, respectively. In the considered context, the higher the SPCC, the better is the quality of the stego-signal or watermarked signal with the modifications to the cover signal becoming imperceptible.

Average Normal Degradation: The term "normal" refers to a geometric object that is perpendicular to a given object. In 3D computer graphics, the normal is used to determine the orientation of a surface with respect to a light source. The average normal degradation over N triangles of a mesh is given by

$$E_{mesh}(\theta) = \frac{\sum_{n=0}^{N-1} \bar{E}_n(\theta)}{N} \tag{6}$$

where $\bar{E}_n(\theta)$ denotes the expectation of the normal degradation of the n-th triangle. Further, θ is the angle between a triangle and its degraded version after modification of the three vertices of this triangle, e.g., caused by data hiding.

Robustness. Robustness refers to the ability to protect a secret object against impairments caused to the stego-object. The impairments can be inflicted by channel noise or common signal processing such as compression, filtering, and coding. Furthermore, some types of attacks from a steganalyst and other illegal entities are also taken into account to measure robustness. The requirement for robustness of data hiding depends mainly on the application. Most watermarking schemes need to achieve high robustness because the integrity of the watermark is required in the authentication process. Changing or losing secret information during processing and transmitting can lead to ineffectiveness of watermarking schemes. High robustness is also needed against attacks aiming to damage operations or stall the availability of a system. However, there exist some watermarking algorithms in which robustness is purposely set to a low level. These are called fragile watermarks which are usually used in lossless signals. Regarding steganography, the requirement for robustness is not as strict as for watermarking techniques. Steganography techniques are based on channel conditions and require only a reasonable level of robustness such that the secret object can be covertly sent from the sender to the receiver where the secret object and the cover object should be successfully recovered. Robustness of data hiding techniques is often evaluated in terms of how they can cope with or resist, e.g., the following impairments:

- Lossy compression such as the MP3 audio format, Joint Photographic Experts Group (JPEG) image format, and the H.264 video format.

- Noise including additive white Gaussian noise (AWGN), salt and pepper noise, Gaussian noise, speckle noise, qubit flip noise, and quantum channel noise.
- Attacks such as pasting, cropping, geometric, noise, frame-based, enhancement, and compression attacks.

Normalized Correlation (NC) [25]: Robustness can be measured by the similarity between two versions of the secret data using the normalized correlation. Given the secret object S and the secret object S_{ext} extracted from the stego-object, the NC between these two objects is defined in general as

$$\mathrm{NC} = \frac{\sum_{n=0}^{N-1} S(n) \cdot S_{ext}(n)}{\sqrt{\sum_{n=0}^{N-1} [S(n)]^2} \sqrt{\sum_{n=0}^{N-1} [S_{ext}(n)]^2}} \tag{7}$$

where $S(n)$ and $S_{ext}(n)$ denote the n-th element of the respective objects each comprising of a total of N elements. For example, an element may be a sample of an audio signal or a pixel of an image or video frame. Depending on the application, the higher the NC, the larger is the robustness of the particular technique in terms of recovering the watermark, recovering the stego-object, or reconstructing the cover object.

Bit Error Rate (BER) and Error Ratio (ER): The BER between a secret object S and the corresponding extracted secret object S_{ext}, both given in binary format, is defined as

$$\mathrm{BER} = \frac{\sum_{n=0}^{N-1} S(n) \oplus S_{ext}(n)}{N} \tag{8}$$

where $\oplus$ denotes the exclusive-or (XOR) operator between the n-th original secret bit and the extracted bit. Some publications use the error ratio which is defined as

$$\mathrm{ER}(\%) = \frac{\sum_{n=0}^{N-1} S(n) \oplus S_{ext}(n)}{N} \times 100 \tag{9}$$

Similar as with the NC, the lower the BER or ER is, the higher is the robustness of the particular data hiding technique.

Detectability. Detectability refers to the ability of a data hiding system to protect a secret message hidden in a stego-object from being detected by a steganalyst [12, 16]. Detectability is not limited to distinguishing between stego-object and cover object like imperceptibility. Although imperceptibility makes detection more difficult, other factors also need to be considered such as the size of hiding space and the strategies used by the steganalyst. For example, even though a data hiding technique may resort on simple operations, the detectability of the hidden data would be negligible if the amount of secret data is sufficiently small compared to the size of the cover object.

The performance of data hiding techniques regarding detectability is often provided in qualitative terms such as resisting or being fragile with respect to specific types of steganalysis:

- Histogram attacks, pixel difference histogram steganalysis, image histograms, visual attacks.
- Statistical moments based steganalysis, second-order derivative-based Mel-cepstrum (3D-Mel) steganalysis, higher order statistics (HOS) steganalysis, similarity measures.
- Steganalysis based on convolutional neural networks, steganalysis in time and frequency domains, regular singular (RS) attack, Chi-square goodness of fit test, S-family-attack resistance test detecting the length of the embedded secret bits.

The detection accuracy is often used as a metric to measure the detectability obtained by a steganalysis method. The detection accuracy is defined as

$$\text{Detection Accuracy} = \frac{TP + TN}{TP + FP + FN + TN} \tag{10}$$

where TP, TN, FP, and FN stand for true positive, true negative, false positive, and false negative predictions, respectively. The true outcomes are the correct predictions while the false outcomes are the erroneous predictions made by the method.

Security. Security measures the ability of protecting secret objects against attacks of a steganalyst such as reading secret content, tampering, reusing, and removing the secret object. Security is the most crucial metric for watermarking techniques while it is not as important as detectability for steganography. Most publications on steganography have considered security of steganography algorithms as being equal to the ability of making the secret object undetectable [12]. The secret object is secure until the stego-object is specified and the hiding places are determined. This is true only for pure steganography which uses simple data hiding without a stego-key. It is not true for many other approaches such as steganography combined with cryptography where the message content is kept secure even when all secret objects are extracted. For watermarking techniques, many studies assume that security is equivalent to robustness. However, attacks of tampering and reusing watermarks cannot be categorized in this way. Encryption techniques used in combination with data hiding techniques include the following:

- Advanced encryption standard (AES), Rivest cipher 6 (RC6), data encryption standard (DES), Rivest-Shamir-Adleman (RSA) encryption, and scrambling of secret data using *m*-sequences.

1.3. Surveys on Data Hiding in Digital Media

In recent years, a number of surveys have been conducted on steganography for digital media such as audio, images, videos, and 3D media. These works provide comprehensive overviews on the state-of-the-art steganography techniques for the respective digital media as follows.

Digital Audio. In [26], a comparative study of digital audio steganography techniques is provided where audio files are used as cover medium. This survey is motivated by the fact that digital audio steganography has become an attractive approach for data hiding in Voice over Internet Protocol (VoIP), audio conferencing and other novel telecommunication technologies. The performance of the steganography techniques reviewed in this article is evaluated in terms of robustness, security, and capacity. The review of audio steganography methods distinguishes between temporal domain, transform domain, and codec based techniques. In the temporal domain, conventional LSB, LSB variants engaging higher bit planes, and silence intervals in speech signals are used for data hiding. The transform domain methods include tone insertion, phase coding, amplitude coding, cepstral domain, spread spectrum, allpass digital filters, and discrete wavelet transform based data hiding. Data hiding in the coded domain resorts on voice encoders such as adaptive multirate (AMR), algebraic code-excited linear prediction (ACELP), and the SILK encoder developed by Skype. In particular, in-encoder techniques embed data into speech and music signals such that they can survive encoding, compression, reverberations, and background noise. Alternatively, post-encoder techniques hide secret data in the bitstream that is generated by the audio encoder. The survey concludes with pointing out several applications and trends such as medical records secrecy, hiding text messages in audio multimedia messages, embedded data transmission over acoustic channels, and data storage.

The first survey dedicated to VoIP steganography and its detection is provided in [27]. It reflects the popularity that this field has gained due to, e.g., the large volume of VoIP data available for data hiding, the potentially high capacity provided, and the resistance against steganalysis because of the dynamic and variable length of VoIP calls. In this survey, VoIP steganography is classified into methods that modify the protocol data unit (PDU) network protocol headers or the payload field, methods that modify the PDU time relations such as PDU interpacket delay, and methods that modify both the content of the PDUs and the PDU time relations. A performance summary of the VoIP steganography methods to the voice payload and to VoIP-specific protocols is provided in terms of undetectability, robustness, and capacity. It is concluded, among others, that future research may be directed toward hybrid methods that modify both VoIP PDUs and their time relations because these methods would offer sufficient capacity while maintaining undetectability. Regarding steganalysis, it is concluded that there is no method that could serve as a universal detection solution.

The monography [28] is dedicated to information hiding in speech signals for secure communications over networks. It gives a comprehensive introduction including methods for hiding secret speech information in different digital speech coding standards, provides an information hiding model for speech secure communication, and information hiding algorithms and techniques for speech communications that are able to resist evolved attacks. Among the variety of information hiding approaches presented in this work, it also discusses the LSB replacement technique in the context of embedding secret speech into G.711 telephony speech, G.721 speech coded formats, and VoIP G.729 speech flows. The performance of speech information hiding algorithms is assessed in terms of security, capacity, and speech quality.

The most recent survey on digital audio steganography in [29] provides a systematic review, classification, and analysis of the state-of-the-art in this field. This survey proposes a classification of digital audio steganography based on the embedding process including linear sequential embedding, selective-based embedding, frequency masking and amplitude thresholding, error minimization-based embedding, pattern-matching-based embedding among others. Due to the choice of classification criteria, this systematic review improves on the segregation level and depth of analysis of the reviewed articles compared to other reviews.

Digital Images. In [30], a comprehensive survey and analysis of steganography methods for digital images are provided. An overview on the different types of information hiding distinguishes between steganography and watermarking along with related nomenclature. The digital image steganography methods discussed in this survey include spatial domain techniques that are centered around LSB replacement techniques, frequency domain methods that utilize Fourier transform (FT), discrete cosine transform (DCT) and discrete wavelet transform (DWT), and adaptive steganography. A performance assessment of the different methods of digital image steganography is mainly conducted using both PSNR and visual inspection. Reference to other similarity measures is also provided. In addition,

a comparison of several software tools for steganography is provided with respect to data hiding in the frequency domain, random bit selection, support for encryption, and supported image formats. This survey also describes some issues and standards related to steganalysis for digital images which attempt to attack steganography methods, e.g., using visual inspection and image histogram characteristics.

A survey on the status and key issues in image steganography is provided in [31] using a classification into spatial domain techniques, transform domain techniques, spread spectrum steganography, and model-based steganography. Apart from LSB data hiding in the spatial domain, major steganography tools that use LSB embedding or replacement in the transform domain are reviewed, i.e., Jsteg/JPHide, F5, and Outguess. Performance assessment of steganography techniques is suggested to consider measures such as security against attacks, capacity, and imperceptibility.

In [32], a survey on watermarking schemes for image authentication is presented including self-embedding based schemes, pixel grouping and probability distribution based schemes, Hamming code based schemes, and transform domain based schemes. Other approaches that do not fall in any of the aforementioned classes of schemes are also provided. A brief overview about attacks on fragile watermarks is also given. Several LSB data hiding techniques are discussed indicating their uses throughout the considered watermarking schemes. This survey also presents metrics for assessing the perceptual quality of watermarked and recovered images, i.e., PSNR, the normalized correlation coefficient, SSIM, and the universal image quality index. Furthermore, three metrics for evaluating the tamper detection performance are described, i.e., probability of false acceptance, probability of false rejection, and probability of false detection. The general conclusion of this survey is that current methods for image authentication and recovery are not perfect which leaves large scope for research on improved watermarking schemes.

In [33], a comprehensive survey of image steganography is provided focusing on techniques, evaluations, and trends in future research. The review commences with an introduction to information security distinguishing between cryptography, steganography, and watermarking. Brief background of steganography is given and the general procedures involved in steganography are discussed. Four attributes of steganography systems are reported to be essential for evaluating and comparing different methods, i.e., imperceptibility, security, capacity, and robustness. The trade-off between attributes of data hiding is used to classify steganography techniques into naïve steganography techniques (capacity of main concern), secure steganography techniques (security of main concern), and digital watermarking (robustness of main concern). Given this background information on steganography, applications and performance evaluation techniques are presented. The latter includes capacity, PSNR, SSIM, and the correlation coefficient between the intensity of pixels in the stego-image and cover image. The image steganography techniques discussed in this survey are classified based on the cover image dimension, the retrieval nature of separating the secret message from the stego-image, and the embedding domain. Specifically, the spatial domain image steganography considers LSB steganography, pixel value differencing steganography, histogram shifting based steganography, difference expansion steganography, multiple bit plane based steganography, palette based steganography, pixel intensity modulation based steganography, and quantization based steganography. Similarly detailed classifications are provided for transform domain image steganography and adaptive steganography. A detailed evaluation of the surveyed image steganography techniques is provided with respect to the spatial domain, transform domain, and adaptive methods. The evaluation includes classifying the specific methods, describing the methods, whether they are reversible or not, their advantages and disadvantages, and results related to capacity and PSNR. In addition, guidelines for selecting cover images are provided which reveal the importance of the cover image in the steganography process of not leaving suspicious noise in the embedded image. It is suggested to embed secret messages in image texture or edge areas rather than smooth areas, use correlation-based cover selection procedures with respect to the similarity of image blocks, or use the Fisher information matrix and Gaussian mixture model for measuring embedding ability. Furthermore, an overview of steganalysis is provided such as signature and statistical steganalysis. Future directions proposed to improve current image steganography techniques include exploring features of the transform domain, using machine learning to optimize adaptive embedding approaches, combining cryptography with steganography, and developing advanced counter measures to deal with attacks on the stego-image.

In [34], a review of recent advances in image steganography is provided. The main aim of this review is on available methodologies and trends, especially, discussing the role of deep learning techniques in image steganography. Accordingly, methods are classified into traditional steganography methods such as LSB data hiding, convolutional neural network (CNN) based methods, and generative adversarial network (GAN) based methods. A number of datasets used in relation to deep learning approaches are also described. The metrics used for performance evaluation are MSE, PSNR, and SSIM relating to imperceptibility, accuracy relating to robustness and security, and bpp relating to capacity. It is concluded that the deep learning methods

may outperform traditional steganography in terms of capacity, security and robustness. However, it is pointed out that the extraction of the secret image is prone to loss of information in deep learning methods. Other challenges of deep learning methods include the lack of benchmark datasets, problems of not converging to a solution, need of other evaluation metrics, and difficulty in performing real-time steganography.

Digital Video. An overview dedicated to information hiding in the H.264/advanced video coding (AVC) format is given in [35]. The discussed information hiding techniques are classified with respect to data representation schemes, namely, bit plane replacement, spread spectrum-based data hiding which is often used with watermarking, histogram manipulation, mapping rules relying on a set of codewords for information embedding, exploiting the divisibility of a value by a specific factor, and their combination with matrix encoding. LSB data hiding is described with respect to bit plane replacement, use in the transform domain, and LSB insertion in the entropy coding. The performance of the considered techniques is assessed qualitatively rather than quantitatively. Recommendations given in this survey include developing a unification of encryption and information hiding in the compressed video domain.

A comprehensive review on video steganography is provided in [36] including some attacks and steganalysis techniques. In this review, the steganography methods are classified into substitution, transform domain, adaptive, format-based, real-time, and cover generation methods. LSB data hiding is described in the context of substitution-based techniques which is noted to be capable of hiding large secret messages in spite of its simplicity. The performance measures reviewed relate to the visual quality of stego-videos and are centered around error-based quality metrics and structural distortions, respectively, i.e., MSE, root mean square error (RMSE), SNR, PSNR, weighted PSNR (WPSNR), SSIM, and the general video quality model (VQM_G). The conclusions provide several recommendations such as integrating of steganography with cryptography, blind data retrieval, working with the color space, and avoiding the use of videos with smooth homogeneous background among others.

In [37], a survey and analysis of video steganography in the compressed and raw domains are provided. The compressed domain considers video steganography in intra-frame prediction, inter-frame prediction, motion vectors, transform coefficients, and entropy encoding. The video steganography techniques are classified with respect to the spatial domain and transform domain. LSB data hiding techniques are presented using motion vectors, transform coefficients, and LSB substitution in the spatial domain for hiding the secret data. The performance of the reviewed video steganography techniques is mainly compared in terms of capacity, video quality, and robustness. The conclusions, among others, suggest developing a video steganography method that can offer a trade-off between video quality, capacity, and robustness against attacks.

In [38], a comprehensive review of video steganography is provided in the context of network transmission. Depending on the embedding position of the secret message, steganography for digital video is classified into pre-embedding, intra-embedding, and post-embedding. In video steganography methods based on pre-embedding, the secret message is embedded in the raw video domain. In these methods, a video sequence is considered as an ordered set of frames in which embedding of secret messages is performed in the spatial or transform domain prior compression. Pre-embedding methods neither depend on the specific video coding process nor affect the use of contemporary video coding standards. LSB data hiding belongs to the prominent video steganography methods used at the pre-embedding stage as it is simple and offers high capacity. Intra-embedding refers to methods that combine video coding and syntax elements which are used at various video processing stages such as intra-prediction, motion estimation, and DCT coefficients. The intra-embedding methods presented in this review are performed in the compressed domain for a given video format, e.g., belonging to the H.26X and MPEG-X families of video compression standards. In post-embedding, the secret message is embedded in the bitstream that has been generated by the specific video codec. In this review, it is suggested to assess the performance of steganography algorithms in terms of imperceptibility, robustness, capacity, and algorithm complexity. Directions for future video steganography are provided including H.265 video steganography, robust video steganography, reversible video steganography, and video steganography based on artificial intelligence.

3D Media. In [39], a survey on 3D image steganography techniques is presented where images are given as mesh models. The approaches for data hiding in 3D images are classified into spatial domain and frequency domain. The spatial domain is further divided into geometrical (changing of geometry such as vertices), topological (modification of the connectivity of vertices), and representation domain steganography (exploiting redundancy contained in the mesh representation). Furthermore, an overview on the types of attacks on 3D mesh models and steganalysis techniques is provided. Regarding LSB data hiding, techniques from 2D images are extended to 3D images such as applying LSB substitution to the vertices of 3D cover mesh models. The performance of the different approaches in the spatial domain is quantified regarding capacity. It is concluded

that 3D steganography and steganalysis are underdeveloped and would therefore require further research.

The review provided in [40] is focused on authentication based watermarking techniques for 3D models in the spatial domain and related geometric mesh attacks. In particular, a generic classification of different fragile mesh watermarking schemes for 3D meshes is provided that is based on attributes of, e.g., reversibility, embedding style, and extraction procedure. A technique related to LSB data hiding is reported that uses simple LSB substitution in the angular vertex coordinates for embedding the watermark. An overview of performance measures is also provided relating to imperceptibility, robustness, and tamper detection. It is concluded that almost all work on fragile watermarking for 3D meshes so far has been focused on the spatial domain. Research on enhancing the effectiveness of authentication schemes for 3D models and tamper recovery for 3D meshes are suggested as future work.

Surveys Dedicated to LSB Data Hiding. The above surveys on data hiding in digital media are dedicated to either digital audio, images, videos, or 3D media while LSB data hiding is covered as one among numerous other approaches. Several conference papers providing surveys that focus on LSB data hiding have been provided as [41–47]. To the best of our knowledge, a comprehensive survey on LSB data hiding that considers digital audio, images, videos, and 3D media does not exist.

1.4. Classification of LSB Data Hiding Techniques

While the surveys discussed in Section 1.3 consider a broad spectrum of digital media data hiding methods, this survey is dedicated to LSB data hiding in digital media. Given the reviewed literature, a classification of LSB data hiding for digital media may be suggested as shown in Fig. 2. The classification of LSB data hiding may rely on the type of digital media, i.e., digital audio, image, video, and 3D media. LSB data hiding for digital audio can be categorized into techniques that hide secret messages in the temporal, transform, and coded domains. Similarly, LSB data hiding for digital images can be classified into techniques that perform the embedding of secret messages in the spatial, transform, and quantum domains. Additional sub-categories can be identified for the spatial and transform domain techniques of image steganography. LSB data hiding for digital videos may be organized into techniques that modify raw data and compressed data with associated sub-categories in each of these two classes. Finally, 3D digital media stands for new digital media such as 3D images, 360° images and videos, and may be extended to immersive media like VR, AR, and future holopresence systems. Current LSB techniques in 3D digital media may be classified into 3D-mesh media, 3D anaglyph media, and 360° media. It should be noted that LSB data hiding for new digital media is currently in its infancy and hence requires increased attention in the coming years to address the security challenges associated with upcoming networked immersive media.

1.5. Motivation and Contributions

With the widespread use of digital media communications over wireless and wired networks, there has been a significantly increasing demand on information security techniques that protect the confidentiality, integrity and availability of the information. The tremendous amount of data hiding techniques for digital media that have been proposed over the years shows its important role in protecting digital media systems. The existing surveys on data hiding for digital media have concentrated on a particular digital media type and reviewed a wide range of information hiding techniques used with the selected type. However, to the best of our knowledge, no comprehensive survey has been dedicated to LSB data hiding considering digital audio, image, video, and 3D media. The proposed survey is therefore focused on LSB data hiding techniques in the aforementioned four types of digital media. The survey significantly expands on our earlier review work on conventional digital images and videos [48] by including digital audio and 3D media, presenting a detailed review of LSB data hiding techniques for each of the four digital media types, summarizing their attributes and performance characteristics, and pointing out future research directions. Based on the above discussion, the major contributions of this survey are as follows:

- The fundamental concepts and terminologies used in data hiding are reviewed along with a general data hiding model.
- The five attributes of data hiding, i.e., capacity, imperceptibility, robustness, detectability, and security, and the related performance metrics used in this survey to compare the characteristics of the different LSB data hiding techniques are discussed.
- A systematic classification of LSB data hiding methods in digital media is presented with respect to digital audio, image, video, and 3D media and the different domains utilized for hiding secret information.
- Based on this classification of LSB data hiding methods, comprehensive surveys of LSB data hiding are provided for each of these four digital media including landmark studies, state-of-the-art approaches, and applications of LSB

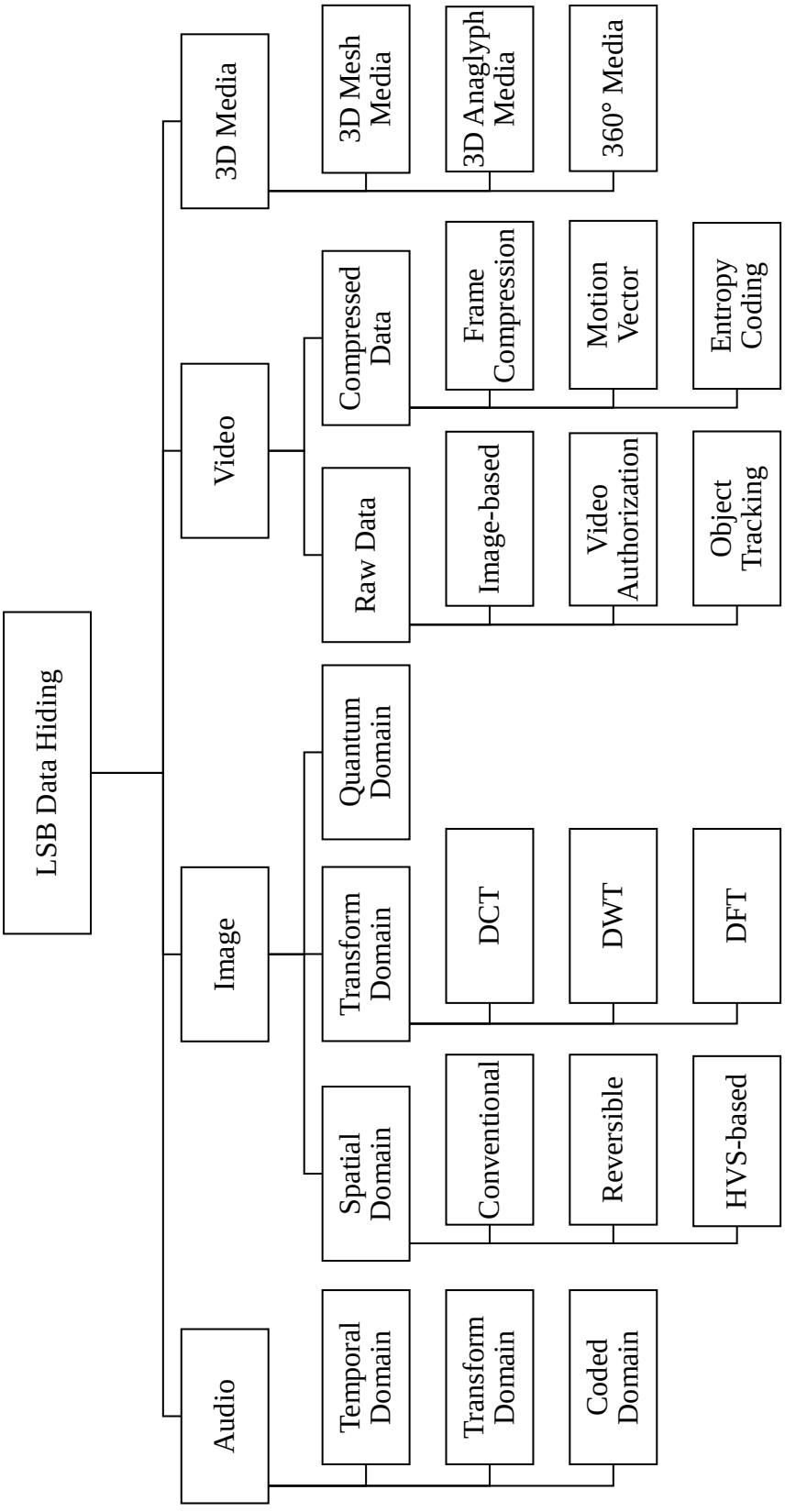

Figure 2. Classification of LSB data hiding techniques for digital media.

data hiding in the respective digital media. Their performance is compared with respect to the considered data hiding attributes which illustrates benefits and drawbacks of the reviewed LSB data hiding methods.

- The survey concludes with summarizing main findings, pointing out challenges, and suggesting directions for future research.

This comprehensive survey will be helpful for researchers and practitioners to keep abreast about the potential of LSB data hiding in digital media and to develop novel applications based on suitable performance trade-offs between different data hiding attributes.

2. LSB Data Hiding in Audio

An audio signal is a representation of voice, speech, music, and all types of sounds within the normal audible hearing range for humans covering frequencies from 20 Hz to 20 kHz. The human voice spans a frequency range from around 125 Hz to 8 kHz when applied to speech. Audio frequencies used for the transmission of speech use voice bands, e.g., frequencies from 300 Hz to 3.4 kHz for narrowband telephony. This section provides a review on LSB data hiding in digital audio using the classification shown in Fig. 2, i.e., considering the temporal, transform, and coded domains.

2.1. Temporal Domain

The first studies on LSB data hiding in the temporal domain of audio samples were proposed more than 30 years ago. A patent using LSB data hiding to protect the copyright of audio stored on compact disc was proposed in 1989 [49]. This method randomly selects samples belonging to a pulse-code modulation (PCM) audio signal. One or more insignificant bits of the selected samples are replaced by pseudo-random bits. The sequence of pseudo-random bits, considered as watermark or identification sequence, is stored to allow subsequent identification of copies of the recorded material. A suspected copy of the recorded material is checked by comparing sequences of digits with the known pseudo-random separation and the stored identification sequence. Based on a selected level of incidence of identical occurrences, the genuine source of the test signal is authenticated. Since then, many advanced data hiding algorithms have been developed to improve capacity, imperceptibility, and other attributes.

In [50], four LSBs per cover audio sample are replaced by four secret bits. Then, minimum-error replacement (MER) based on the comparison between replacing k LSBs and flipping only the $(k+1)$-th LSB of a sample is used to find the level of the stego-sample closest to the original audio level. This method keeps the SNR close to that of standard LSB replacement but achieves 33% higher capacity. Similarly, the LSB data hiding algorithm proposed in [51] is even applied to the sixth or seventh LSB for robust audio watermarking. The $(k+1)$-th bit plane covers the authentication bits, and the lower-order bits are modified to reduce the change of the audio samples. Error diffusion is performed to shape the impulse noise caused by the data hiding to a perceptually more favorable distribution. The secret bits hidden in the high bit planes are robust against additive noise. Steganalysis is more challenging compared to standard LSB data hiding because the bit planes used for data hiding cannot exactly be identified.

Another solution to minimize audio degradation subject to a given capacity target is to apply optimization methods to find substitutions with the least difference to cover audio samples. In [52], six bit planes are selected randomly ranging from the LSB to the tenth LSB of 16-bit samples in waveform audio file (WAV) format. The secret bits are embedded into selected bit planes, and the obtained values of the audio samples before and after modification are compared. This process is iterated 100 times to find the best substitution that gives the most negligible difference between the original samples and the stego-samples. As a result, the stego-samples achieve the highest quality in terms of SNR for a given capacity target. Instead of iterating many times over randomly selected bit planes to find the best result, genetic algorithms (GAs) are proposed in [53, 54]. Data hiding is performed in each cover audio sample, and the stego-sample is considered as a chromosome containing a sequence of bits. Each chromosome can create many different chromosomes through crossover and mutation. New chromosomes are generated several times until a satisfactory result closest to the value of the cover sample is obtained, and this result is kept as the final stego-sample. This GA-based data hiding process is continued for the rest of the audio samples. LSB data hiding with syndrome-trellis code (STC) is another approach to improve security and minimize distortions caused by data hiding in audio samples. A conventional STC-based data hiding algorithm uses a parity-check matrix created from a fixed sub-matrix for the whole embedding and extraction process [55]. The work in [56] makes further improvement with an adaptive parity-check matrix consisting of many sub-matrices whose sizes vary according to the complexity of the audio samples.

Many studies combine scrambling techniques and cryptography algorithms with LSB data hiding to strengthen security. In [57], Euler's three-body chaotic model is used to scramble the indices of selected audio samples to complicate the retrieval of the secret

bits without having the proper stego-key. Similarly, the steganography model in [58] uses the logistic map for randomizing hiding positions to enhance security. To achieve confidentiality and integrity of audio streams, the LSB watermarking in [59] uses a hash function and symmetric cryptography. Each user is associated with the 128-bit MD5 [60] hash value of a selected unique image from a private database. The audio signal of an authorized speaker is watermarked using LSB replacement with the related hash value to check integrity. Then, the watermarked audio signal is encrypted using the AES [61] or RC6 [62] algorithms to provide confidentiality.

With the development of quantum technology that allows audio signals to be presented and processed in qubits, many researchers have extended LSB data hiding into the temporal domain of audio quantum formats. In [63], two data hiding protocols are implemented with a circuit model of quantum computation. The first protocol substitutes the least significant qubits (LSQb) of the cover quantum audio signal with the secret qubits of a quantum audio message. In contrast, the second protocol selectively alters the most significant qubit (MSQb) of the cover quantum audio. The former technique achieves higher imperceptibility but is less robust than the latter approach. Another audio watermarking technique is proposed in [64] to protect the copyright of audio in quantum networks. An image, considered as secret data, is scrambled and embedded into either the LSQb or second LSQb of an audio signal in the quantum domain. The bit planes used for data hiding depend on the value of the MSQbs of the audio samples.

Table 1 summarizes the performance of the above studies on LSB data hiding in the temporal domain with respect to the considered five data hiding attributes. The advantage of LSB data hiding in the temporal domain is that it provides large capacity within an acceptable level of impairments to the cover object. Another advantage is that a suitably designed data hiding algorithm in combination with other techniques such as cryptography can improve undetectability and strengthen security. However, the reviewed LSB data hiding techniques are hardly able to preserve the hidden data under noise and data processing. Although using higher bit planes for data hiding may improve resistance against additive noise, low robustness is a drawback of LSB data hiding in the temporal domain.

2.2. Transform Domain

In this domain, LSB data hiding is performed on the binary representation of the transform coefficients obtained by a particular transformation technique. Because each transform has its own features of presenting audio samples, there exist many options of applying LSB data hiding to the transform domain.

DWTs, which decompose signals into lowpass and highpass components, are most frequently used for LSB data hiding. In [65], an LSB steganography algorithm is proposed using DWT with a one-dimensional Haar filter and perfect reconstruction filters. Each set of 512 audio samples is transformed into a corresponding set of 512 DWT coefficients. All DWT coefficients are used to cover secret bits applying LSB replacement where each of the 16-bit DWT coefficients can use a maximum of 8 LSBs for data hiding. The proposed approach outperforms classical LSB data hiding in the temporal domain by 150-200 kbps capacity for the same SNR while maintaining high subjective quality. The works in [66, 67] apply DWT to the cover speech samples and the secret message, e.g., another speech signal also known as embedded speech-in-speech hiding. Both 16-bit cover speech samples and 8-bit secret message are transformed to approximation or coarse coefficients and detail coefficients. While all coefficients of the cover speech samples are used for data hiding, only the coarse coefficients of the secret message are kept and sorted by a permutation key. The sorted coarse coefficients of the secret message are hidden in the coarse coefficients of the cover audio, and the permutation key is covered in the detail coefficients of the cover speech samples. An inverse DWT then transforms the stego-coefficients to the stego-samples in the temporal domain. These approaches support secure and high quality speech transmission, allow real-time processing, and recover the secret message close to the original one. Because the DWT coefficients are not integers, they need to be scaled and then converted to binary words before covering secret bits. In [68], an LSB-based audio steganography method in the integer wavelet domain is proposed which covers wavelet coefficients into integer coefficients with the number of bits confined by the hearing threshold. Another solution is to use a lifting wavelet transform (LWT) where the resulting coefficients are directly obtained as integers that can cover secret data without any further processing. The work in [69] replaces the DWT with the LWT for LSB data hiding, and the LSBs of the LWT coefficients are used to conceal encrypted data. This work uses threshold calculation which controls the number of secret bits to be hidden according to the frequency range of the subbands. As the HAS cannot discern sounds at very low or high frequencies, the high- or low-frequency coefficients are used to embed more secret bits compared to the moderate frequency coefficients.

The DCT has also been widely used for LSB data hiding in audio. In [70], blind audio LSB watermarking is performed using DCT coefficients. The M samples of the cover audio are divided

Table 1. Performance of LSB data hiding in the temporal domain of audio

Reference	Capacity	Imperceptibility	Robustness	Detectability	Security
[50]	176.4 kbps[1]	SNR ≥ 40 dB MOS ≥ 4.8	–	–	–
[51]	44.1 kbps	SNR > 50 dB MOS ≥ 4.6	resists AWGN	–	selects dynamically LSB layer used for data hiding
[52]	6 bits/sample	SNR ≥ 60 dB	–	–	compresses and encrypts secret data
[54]	4 bits/sample	SNR ≥ 55 dB	–	–	–
[56]	0.4 bit/sample	SI–SNR ≥ 75 dB	–	resists steganalysis based on convolutional neural network	–
[57]	–	MOS > 3	fragile under AWGN and lossy compression	–	controls the number of bit planes used
[58]	1 bit/sample	SNR ≥ 70 dB PSNR ≥ 99.5 dB	–	resists histogram attack, statistical moments based steganalysis	uses chaotic hiding positions
[59]	1 bit/byte	SD > 30 CORR > 0.9994	–	–	uses MD5 hash function and AES/RC6 encryption
[63]	1 qubit/sample	SNR ≥ 50 dB	resists AWGN with BER ≤ 0.5	–	–
[64]	1 qubit/sample	SNR ≥ 45 dB	–	–	scrambles secret data and uses dynamic stego-key

[1] The studied audio signal is a 16-bit PCM signal with a sample rate of 44.1 kHz

into N non-overlapping blocks and a synchronization code (12-bit Barker code) used in each block for alleviating attacks such as cropping and editing. The first N samples of each block directly cover the N synchronization bits in the temporal domain. The remaining $M - N$ samples are transformed into DCT coefficients of which the direct current (DC) and low-frequency alternating current (AC) coefficients contain Bose–Chaudhuri–Hocquenghem (BCH) [71] coded bits of the watermark data. Experimental results reveal that the hidden watermark is robust to attacks caused by additive noise, MP3 coding, and cropping while the BCH code lowers the error rate in the watermark extraction. In [72], two variants of an LSB watermarking algorithm using a modified discrete cosine transform (MDCT) [73] and DCT are compared. Blocks of the original audio signal in the time domain consisting of 512 samples are transformed into corresponding frequency coefficients by either MDCT or DCT. The low-frequency coefficients are selected to cover the secret bits because they are less sensitive to attacks such as compression than the high-frequency coefficients. The strong tonal components residing in the low-frequency coefficients are specified by the psychoacoustic model 1 of the MPEG1 standard which operates on blocks of 384 coefficients. The LSB substitution is performed in the frequency coefficients of these tonal components with a (12,8) Hamming code used to protect the watermark allowing for correction of erroneous bits if needed. While MDCT and DCT achieve high capacity and good imperceptibility, MDCT provides slightly stronger robustness against attacks. Apart from DWT and DCT, some types of the Fourier transform are also applied in LSB data hiding methods. In [74], LSB data hiding using the fast Fourier transform (FFT) is proposed. The FFT converts speech samples into magnitude and phase components of frequency domain coefficients to increase the capacity and security of the embedded information. High energy magnitude frequency components with respect to a given threshold and distortion level are selected for data hiding. In addition, LSB data hiding in phase components and hybrid data hiding in magnitude and phase are also considered. It is concluded that the proposed methods achieve good results regarding capacity and security against the Fourier spectrum statistics based steganalysis proposed in [75]. Several variants of the Fourier transform, including discrete Fourier transform (DFT), fractional Fourier transform (FrFT), and quaternion discrete Fourier transform (QDFT), are used to process a cover audio signal [76]. Two LSB methods are performed to watermark the real part of high-frequency coefficients resulting from the three Fourier transforms. The first method uses three coefficients to cover two secret bits while the second method requires two coefficients to insert one secret bit. The conclusion is that the former method is suitable to the QDFT coefficients while the latter offers good imperceptibility for data hiding in DFT and FrFT coefficients.

Some studies combine different transforms or a particular transform with other types of data processing to

improve the LSB data hiding performance. In [77], DWT and DCT are combined to improve the transparency and robustness of digital audio watermarks against synchronization attacks. Each audio segment of the cover signal is first transformed using the DWT, resulting in a coarse coefficient (low-frequency) and detail coefficients (high-frequency) while the DCT is performed only on the coarse coefficients. The encrypted watermark bits are embedded into the magnitude of the DCT coefficient by quantization to guarantee robustness and transparency. In addition, a synchronization code (16-bit Barker code) is embedded in the mean values of all samples of the audio segment to cope with synchronization attacks. This approach significantly reduces audio degradation and considerably strengthens the robustness of the watermark against attacks such as re-sampling, re-quantization, additive noise, cropping, and MP3 compression. Furthermore, the Schur decomposition can be performed with either DCT or DWT coefficients in audio LSB data hiding as described in [78] and [79], respectively. In these works, the Schur decomposition is used to achieve perceptual transparency of audio watermarking. The two proposed watermarking algorithms follow a similar process: Convert the audio signals into the respective transform domain, apply the Schur decomposition, hide one secret bit into the seventh LSB of selected coefficients, and reconstruct the audio signals in the temporal domain. The algorithm described in [78] utilizes the mid frequency DCT coefficients while the algorithm suggested in [79] selects the second subband (HL2) of 2-level 2D-Haar DWT coefficients. The DCT-Schur decomposition based watermarking algorithm achieves higher capacity than the DWT-Schur decomposition algorithm, but has lower imperceptibility and robustness. Another example of combining a transform with other techniques is the work reported in [80] which involves performing a fast greedy adaptive dictionary learning (GAD) algorithm with DWT coefficients. The speech signal is divided into many frames, and all frames are transformed into low-frequency and high frequency coefficients using the Haar DWT. The GAD algorithm estimates a dictionary from the high-frequency components of all frames over which the low-frequency components will be represented sparsely. The low-frequency coefficients of high energy frames are selected for data hiding and represented by a set of structural elements using the estimated dictionary. The LSBs of the fractional part of the non-zero elements of the sparse representation are substituted by a secret bit while the integer part of these elements remains unchanged. The stego-frames are reconstructed from its sparse representations by the inverse processes and combined with intact speech frames to produce the stego-speech signal sent to the receiver.

Table 2 summarizes the insights on the attributes and performance of LSB data hiding techniques in the transform domain of audio. Although LSB data hiding in the transform domain improves imperceptibility, capacity is generally limited and lower than in the temporal domain. On the other hand, transform-based LSB data hiding has advantages in terms of robustness and detectability. A gap in these studies is the lack of approaches on security related to confidentiality and integrity which are as important as detectability.

2.3. Coded Domain

This section describes LSB data hiding in speech signals for the two most common approaches of speech processing, i.e., waveform and parameter coding.

In waveform coding like G.711 [84], encoded speech samples can be used for data hiding similarly to raw PCM audio samples in the temporal domain. In [85, 86], LSB data hiding algorithms for VoIP are proposed that use 8-bit speech samples of an encoded frame to conceal the pitch waveform replication data of the previous speech frame. This technique allows to reconstruct lost or delayed packets at the receiver and to improve the speech quality of VoIP, especially, in a high error rate environment. Similarly, in [87], a secret message is hidden in a cover speech signal using the so-called LSB matching (see Section 3.1). The stego-signals are encapsulated and transmitted by the real-time transport protocol (RTP). Furthermore, a mechanism for exchanging information and re-transmission of secret data contained in lost packets is defined so that the lost secret data is re-embedded into a new speech packet. In [88], high quality speech transmission through a narrow bandwidth channel is proposed by using LSB data hiding in the coded domain. The speech signal is first divided into low-frequency and high-frequency components. The low-frequency component is encoded by an G.711 encoder. The high-frequency component produces 66-bit parameters for each speech frame, which are considered as secret data, compressed, and embedded into the G.711 bitstream using a modified watermark method. The resulting bitstream is transmitted to the receiver through a narrowband channel. At the receiver, the low-frequency component is decoded with a G.711 decoder while the high-frequency component is extracted from the received bitstream. The wideband speech is finally synthesized by combining these two frequency components.

With parameter coding, different standards define different sets of parameters that characterize audio frames. Therefore, LSB data hiding methods have to use suitable parameters such that the impact of the modifications on the audio quality is kept low. For example, the G.792 standard [89] encodes each frame of 80 audio samples into 80 bits consisting of parameters

Table 2. Performance of LSB data hiding in the transform domain of audio

Reference	Capacity	Imperceptibility	Robustness	Detectability	Security
[65]	8 bits/sc	SNR ≥ 40 dB, MOS ≥ 4.5	–	–	–
[66]	8 bits/sc	–	–	passes steganalysis in time and frequency domains	scrambles secret bits
[67]	8 bits/sc	SNR = 33.88 dB, SPCC = 0.999	SNR = 16.65 dB, SPCC = 0.978	–	–
[68]	296.35 kbps[1]	SNR ≥ 38 dB, MOS ≥ 4.7	full recovery, BER = 0	–	–
[69]	239.79 kbps	SNR ≥ 33 dB, MOS ≥ 4.7	full recovery, BER = 0	–	–
[70]	–	–	robust against noise and MP3 compression	–	–
[72]	109.28 - 278.18 bps	SNR ≥ 60 dB ODG ∈ [−0.2, 0]	resists attacks of Stirmark [81] and MP3 compression	–	–
[74]	25.1 kbps	SNR ≥ 30 dB	–	resists steganalysis in [75]	–
[76]	1st variant: 2 bits/3 sc, 2nd variant: 1 bit/2 sc	SNR ≥ 35 dB CORR ≥ 0.9995	NC > 0.9 under certain attacks[2]	–	–
[77]	1 bit/byte	–	NC ≥ 0.93, BER < 0.08 under certain attacks[2]	–	–
[78]	516.26 bps	SNR = 77.95 dB ODG = 0.179	NC ≥ 0.96, BER ≤ 0.054 under certain attacks[2]	–	–
[79]	319.29 bps	SNR = 81.43 dB ODG = 0.184	NC ≥ 0.99, BER ≤ 0.014 under certain attacks[2]	–	–
[80]	1.8 kbps	SNR ≥ 30 dB PESQ > 3.6	–	resists 2D-Mel [82] and the HOS [83] steganalysis	–

[1] The reference audio signal is a 16-bit PCM audio with a sampling rate of 44.1 kHz

[2] Re-quantization, re-sampling, additive noise, and MP3 compression attacks

that vary in bit length and importance. The works in [90–92] consider the parameters of the fixed codebook in G.792 as the least significant parts of a speech frame and apply LSB substitution into the related positions in the codebook. The work in [93] considers parameters of the adaptive-codebook delay and the second stage higher vector of linear spectrum pair quantizer as the least important parts of each speech frame. An LSB embedding method using three-layer modification in these two parameters is designed for low bit rate speech streams. This method enhances capacity while maintaining good perceived speech quality. In [94], the so-called random LSB method (R-LSB) is used to hide a secret speech bitstream coded by a mixed excitation linear prediction (MELP) coder into the cover speech.

Table 3 summarizes the characteristics of LSB data hiding in the coded domain of audio. Clearly, LSB data hiding in the coded domain generally offers only low capacity and weak robustness but maintains acceptable audio quality. However, the detectability in this domain is quite low, and is even boosted by the enormous number of frames and packets exchanged through communication networks. Security can also be achieved in combination with other techniques like cryptography and scrambling algorithms. Although being not as popular as the temporal and transform domain, LSB data hiding in the coded domain plays still a role and has potential applications in speech transmission.

2.4. Applications

In this section, we present applications of LSB data hiding in audio including digital media content protection, VoIP, security for IoT devices, and secure storage.

Digital media content protection: Watermarking has been widely used to provide media content protection. In [96], an LSB data hiding technique is applied to a source coding scheme for authenticating content of 16-bit raw audio signals. This approach achieves high capacity using 4 LSBs, maintains the ability of self-recovery, and resists several attacks including counterfeiting attack, parity bits attack, and key exhaustion attack. Similarly, an LSB fragile watermarking technique is proposed in [97] for encrypted speech data encoded with G.723 standard.

VoIP: In [98], an LSB steganography algorithm is implemented with LinPhone [99] which is an open-source platform for VoIP applications. This work focuses on reducing detectability by dynamically selecting hiding bit planes in a conversational period of an audio stream while the distortion is minimized by adjusting the neighbor of an embedded bit if necessary. A real-time covert channel with strong confidentiality via VoIP communication is proposed in [100]. The secret message is encrypted with AES-128 [61] before being transmitted, and the session key is exchanged

Table 3. Performance of LSB data hiding in the coded domain of audio

Reference	Capacity	Imperceptibility	Robustness	Detectability	Security
[85]	26 bits/frame[1]	SNR = 53.15 dB, PESQ = 4.49 (without packet loss)	–	–	–
[86]	14 bits/frame[1]	SNR = 37.47 dB, PESQ = 4.142	–	–	–
[88]	66 bits/frame[1]	SNR = 34.71 dB	–	–	–
[90]	26 bits/frame[2]	MOS ≥ 3	–	–	encryption with m-sequence and RSA key agreement
[91]	16 bits/frame[2]	MOS ≥ 3	–	–	–
[92]	6 bits/frame[2]	MOS-LQO ≥ 2.5	–	–	encryption with m-sequence
[93]	166.6 bps	PESQ ≥ 3	–	average detection accuracy of steganalysis in [75] = 51.96 %	–
[94]	266.64 bps	PESQ ≥ 2.4	–	average detection accuracy of steganalysis in [95] ≤ 58 %	–

[1] The reference audio signal has a frame rate of 50 frame/s, each frame contains 160 samples of 20 ms length, 8 bits/sample

[2] The reference audio signal has a frame rate of 100 frame/s, each frame contains 80 bits of 10 ms length

by a protocol-based authentication method in the initialization process.

5G networks and IoT: With the development of 5G mobile networks and the widespread use of IoT devices, LSB data hiding has many potential applications due to its low computational complexity. In [101], a speech watermarking algorithm is designed to insert a binary logo into speech signals before passing through filter bank multicarrier modulation. It aims to provide authenticity and integrity of 5G services such as big data, cloud services, and machine-to-machine (M2M) communication. The low computational complexity of LSB data hiding is also attractive to provide secure data communication for smart IoT devices and sensors using audio steganography as suggested in [102]. This application hides data in a random selection of bit planes ranging from the second to the sixth LSB.

Secure storage: Data storage also benefits from LSB data hiding because of the supported high capacity. For example, in combination with the RSA encryption, a text message is stored safely in a personal computer with the help of audio steganography in [103]. Similarly, a secure cloud computing framework is proposed for cloud data security in [104] where the text is encrypted with AES before being distributed into several audio files saved in the multi-cloud.

3. LSB Data Hiding in Images

A review of LSB data hiding methods for images is provided in this section with respect to the classification shown in Fig. 2. Accordingly, LSB data hiding in images may be classified into spatial domain, transform domain, and quantum domain.

3.1. Spatial Domain

LSB data hiding in the spatial domain may be further classified into conventional, reversible, and HVS based methods.

Conventional LSB Data Hiding. The most common forms of conventional LSB data hiding are LSB replacement and LSB matching.

LSB Replacement: This technique simply substitutes the LSBs of the intensity values of a cover image by the bits of a secret message [105]. Apart from using only the LSB for data hiding, two or more bit planes of a given bit width may be used if additional capacity is needed. Many approaches have been developed to improve the performance of LSB replacement in image such as the following. In [106], capacity evaluation based on contrast and luminance measurement is used first to estimate the maximum capacity that can be embedded in each pixel. Second, MER is used to find a gray-scale as close as possible to the original image. Third, improved gray-scale compensation (IGSC) is applied to eliminate the false contouring effect. This approach maximizes capacity while maintaining acceptable image quality. In [107–109], metaheuristic inspired optimization algorithms such as GA and the artificial bee colony algorithm are used to reduce the number of modified pixels. Other methods consider adjusting the pixel intensities of the stego-image to mitigate the impairment caused by the modification of the LSBs [110–112]. To reduce the detectability of the performed LSB replacements, randomizing the pixel positions of the cover image with chaotic maps is proposed in [113, 114], encoding the cover image with a local binary pattern before hiding secret bits is suggested in [115], and combining LSB replacement with other techniques such as the pixel value differencing (PVD) method is used in [116, 117].

LSB Matching: This approach first makes an individual comparison between the LSBs of the cover image and the bits of the secret message [118]. If the LSB of the intensity value of a given pixel of the cover image is equal to the secret bit to be hidden in this pixel, no modification is performed. Otherwise, the respective intensity value of the cover image is increased or decreased by one. The number of increased and decreased intensity values of the cover image is kept balanced such that the LSB modification can be considered as random noise. This balancing is achieved by using bits generated from a pseudo-random sequence generator. LSB matching has been proven to protect the secret message contained in a stego-image from some statistical attacks better than LSB replacement [119].

Another version of LSB matching, called LSB matching revisited (LSBMR), is proposed in [120]. This algorithm embeds a pair (m_i, m_{i+1}) of secret bits m_i and m_{i+1} into a pair (x_i, x_{i+1}) of cover image pixel intensities x_i and x_{i+1}. The i-th secret bit is compared to the LSB of the i-th pixel while the $(i+1)$-th secret bit is compared to the value of a binary function $f(x, y)$ defined as follows:

$$f(x, y) = LSB\left(\left\lfloor \frac{x}{2} \right\rfloor + y\right) \tag{11}$$

where operator $LSB(a)$ returns the LSB of an integer a and $\lfloor b \rfloor$ denotes the floor function which gives the greatest integer less than or equal to the input value b. Then, a pair (y_i, y_{i+1}) of modified intensities y_i and y_{i+1} forming the i-th and $(i+1)$-th pixel of the stego-image is obtained using an LSB modification that distinguishes the following four cases:

- Case 1: $m_i = LSB(x_i)$ and $m_{i+1} = f(x_i, x_{i+1})$ $\Rightarrow y_i = x_i, y_{i+1} = x_{i+1}$
- Case 2: $m_i = LSB(x_i)$ and $m_{i+1} \neq f(x_i, x_{i+1})$ $\Rightarrow y_i = x_i, y_{i+1} = x_{i+1} \pm 1$
- Case 3: $m_i \neq \text{LSB}(x_i)$ and $m_{i+1} = f(x_i - 1, x_{i+1})$ $\Rightarrow y_i = x_i - 1, y_{i+1} = x_{i+1}$
- Case 4: $m_i \neq \text{LSB}(x_i)$ and $m_{i+1} \neq f(x_i - 1, x_{i+1})$ $\Rightarrow y_i = x_i + 1, y_{i+1} = x_{i+1}$

Given the processing according to the above four cases, LSBMR reduces the number of modifications inflicted on the cover image compared to the original LSB matching which results in improved quality of the stego-image and reduced detectability of the hidden secret message.

In [121], in order to further improve embedding efficiency, LSB matching and LSBMR are generalized to the so-called generalized-least significant bit matching (G-LSB-M) algorithm which uses the sum and difference covering all subsets of the finite cyclic group of order

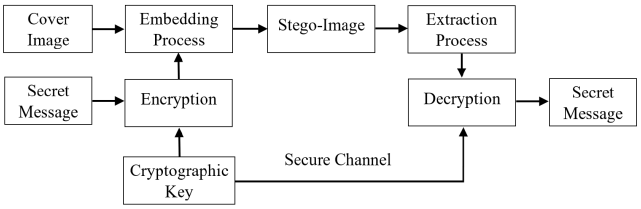

Figure 3. LSB data hiding in combination with cryptography.

2^n. In this algorithm, each element of the finite cyclic group represents n intensities of the cover image, and the secret data is also divided into streams of n bits. It is shown that the G-LSB-M algorithm can further improve the embedding efficiency and offer more secure data hiding in terms of the probability of detection of the secret message compared to LSB matching and LSBMR. It should be mentioned that the expected number of modifications per pixel (ENMPP) is reduced from 0.5 for LSB matching ($n = 1$) and 0.375 for LSBMR ($n = 2$) to 0.333 for G-LSB-M ($n = 3$).

To better protect the confidentiality and integrity of secret messages, some studies propose adding cryptography to LSB data hiding schemes as illustrated in Fig. 3. Instead of directly embedding the secret message, an encrypted version of the secret message is produced and then hidden in the cover image. In addition, a cryptographic key is conveyed to the receiving end through a secret channel to be used for the decryption of the secret message. In [122], an invisible watermarking scheme is proposed which combines LSB data hiding with a hash function and symmetric cryptography. All the LSBs of the cover image pixels are cleared first to ensure that the LSB modification does not affect the calculation of the hash values at the sender and receiver. The modified cover image and a fixed binary watermark image are divided into same-size blocks. The sender applies the MD5 hash function [60] to the blocks of the cover image with a secret key and the resulting hash values are XORed with the corresponding blocks of the watermark image. The final watermark blocks are filled into LSBs of the respective cover blocks. At the receiver, the integrity of every block in the stego-image is checked by comparing the hash value that has been calculated from the cover image by the sender and the hash value calculated from the stego-image with the same secret key at the receiver. This authentication watermarking scheme is extended to the public key system in [123] where a pair of public and private keys replace the pair of the secret keys. Another watermarking scheme in combination with cryptography is described in [124] in which block-based binary logos are used instead of a static mark. Each logo is specialized for a block of the cover image by including the block position, image index, resolution, camera identity (ID), author ID, and

several random bits. Therefore, this scheme can check the authenticity of secret content, the positions of the blocks, and other related information. In [125], elliptic curve public-key cryptography (ECC) is performed within the LSB data hiding scheme. The secret message is transformed into coordinates of elliptic curve points which are encrypted with a public key and then used as input to the embedding process on the cover image. At the receiver, ECC encrypted coordinates of points are extracted from the stego-image and decrypted. In the worst case that the LSB data hiding is detected and all LSB bits are extracted, the attacker only obtains meaningless coordinate points and cannot decrypt the secret message. Thus, a higher level of security is achieved with this method.

Reversible LSB Techniques. The class of reversible LSB techniques relates to the ability to reconstruct the cover image from the stego-image. During the hiding process, the conventional LSB methods do not conserve the LSB values of the cover image. Therefore, the cover image cannot be perfectly recovered from the stego-image. However, many applications require strictly the exact recovery of the cover image at the receiver such as medical imagery or military reconnaissance images. In the spatial domain, several studies have been conducted to deal with this problem using reconstruction data attachment and dual-imaging methods.

Reconstruction Data Attachment: In this approach, the information needed for the reconstruction of the cover image is compressed, attached to the secret message, and embedded into the cover image. The very early reversible LSB data hiding invented in [126] convolves the meta-data related to a cover image with a carrier signal to form a scrambled image which is then used as a secret watermark. The stego-image is a sum modulo N of the secret watermark and the cover image where $N = 2^n$ for a bit width of n. At the receiver, the embedded watermark is extracted first from the stego-image through cross-correlation with the carrier signal. Then, the recovery of the cover image is performed by modulo N subtraction of the watermark from the stego-image.

Another reversible data hiding technique with generalized LSB (G-LSB) modification is proposed in [127] and further developed in [128].

Let the cover image signal be represented by the vector

$$\mathbf{c} = Q_L(\mathbf{c}) + \mathbf{r} \tag{12}$$

where $\mathbf{r} = \mathbf{c} - Q_L(\mathbf{c})$ is the residual vector and $Q_L(\mathbf{x})$ denotes an L-level scalar quantization function

$$Q_L(\mathbf{x}) = L\left\lfloor \frac{\mathbf{x}}{L} \right\rfloor \tag{13}$$

and the floor function $\lfloor a \rfloor$ performs the truncation of the argument a to its integer part. Given a cover image

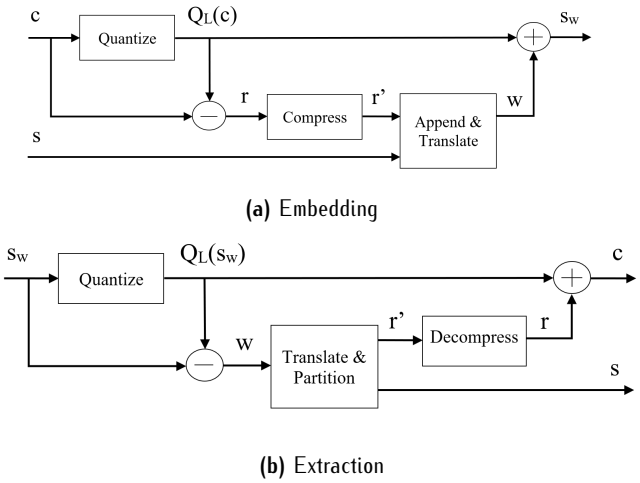

Figure 4. Reversible data hiding using G-LSB modification ©[2005]IEEE. Reprint, with permission, from [127].

$\mathbf{c}$, the G-LSB embedding shown in Fig. 4 (a) substitutes the values of the residual vector $\mathbf{r} = \mathbf{c} - Q_L(\mathbf{s})$ by a watermark vector $\mathbf{w}$ to produce a stego-image as

$$\mathbf{s}_w = Q_L(\mathbf{c}) + \mathbf{w} \tag{14}$$

where the i-th element $w_i \in \{0, 1, ..., L-1\}$ of $\mathbf{w}$ represents an L-ary symbol. Here, a compressed version $\mathbf{r}'$ of the residual vector $\mathbf{r}$ is appended to the secret message $\mathbf{s}$ to make a watermark $\mathbf{w}$ which is to be covered in $Q_L(\mathbf{c})$ by G-LSB data hiding. In the extraction process, as illustrated in Fig. 4 (b), the watermark $\mathbf{w}$ is calculated as

$$\mathbf{w} = \mathbf{s}_w - Q_L(\mathbf{s}_w) = \mathbf{s}_w - Q_L(\mathbf{c}) \tag{15}$$

and partitioned into compressed residual vector $\mathbf{r}'$ and secret message $\mathbf{s}$. The compressed residual vector $\mathbf{r}'$ is decompressed into the residual vector $\mathbf{r}$ which then allows to reconstruct the cover image from the stego-image $\mathbf{s}_w$ as

$$\mathbf{c} = Q_L(\mathbf{s}_w) + \mathbf{r} \tag{16}$$

Dual-imaging Method: The idea of using two identical versions of the cover image in designing a reversible data hiding scheme has originally been proposed in [129]. This method substitutes a pair of pixels in two identical cover images for pairs in two different sets. The two sets have only one common point which is the original pair of pixels in the cover images. Whatever the intensities are changed in the stego-images, the original pair of pixels in the cover image is fixed because it is the intersection of two substitution sets. At the beginning of the recovery process, the pairs of stego-images are used to specify the substitution sets. The pairs of pixels in the cover image can be calculated from the common point of the two substitution sets.

In [130], the LSB matching method is explored as a modification rule for a dual-imaging method as follows. LSB matching is first implemented simultaneously with pairs of pixels $(x_{i,j}, x_{i,j+1})$ and $(y_{i,j}, y_{i,j+1})$ belonging to the first and second cover image with two pairs of secret bits (s_1,s_2) and (s_3,s_4), respectively. Subsequent to the embedding process, the modified pairs of pixels $(x'_{i,j}, x'_{i,j+1})$ and $(y'_{i,j}, y'_{i,j+1})$ are checked whether a pair of original pixels can be restored by performing the floor function on average pixel values as

$$\begin{aligned} p_{(i,j)} &= \left\lfloor \frac{x'_{i,j} + y'_{i,j}}{2} \right\rfloor \\ p_{(i,j+1)} &= \left\lfloor \frac{x'_{i,j+1} + y'_{i,j+1}}{2} \right\rfloor \end{aligned} \tag{17}$$

If $x_{i,j} = p_{i,j}$ and $x_{i,j+1} = p_{i,j+1}$, the modified pairs of values $(x'_{i,j}, x'_{i,j+1})$ and $(y'_{i,j}, y'_{i,j+1})$ serve as the intensity values of the stego-image. Otherwise, a table specifying the modification rule is used to decide the final intensity values of the stego-image.

In [131], the LSB data hiding with dual-imaging method is improved with two layers of security. First, the LSBMR algorithm is performed with pairs of secret bits and pairs of pixels of the cover image. The resulting image is then duplicated and considered as an input of the dual-imaging LSB matching method.

HVS-Based LSB Techniques. Human perception of an image depends on the processing of many visual cues. The image intensity, quantified by the numerical values of the individual pixels of an image, may be considered as one of the most important characteristics of an image as it directly conveys image structures such as objects, characters, landscapes, and other structural information. Other aspects such as color, texture of surfaces, sharpness, size of objects, and image orientation play a considerable role in how humans perceive and assess image quality. Therefore, LSB data hiding techniques have been proposed to take these HVS related aspects into account.

Edge-Based: Depending on the change of intensity values, image regions may be classified into smooth and edge areas (edge and its close surroundings). While a smooth area is characterized by little or no change in intensity values, an edge area shows sharp changes in pixel intensities. Because the HVS is more sensitive to impairments induced to smooth areas compared to edge areas, data hiding in the latter is more beneficial with respect to conserving image quality and reducing visual detectability. In this context, detecting edges in an image becomes an essential part of the development of LSB data hiding techniques that take advantage of the HVS being less affected by modifications in edge areas.

Several works distinguish between edge and smooth areas by directly considering the change in intensity values as follows. The method in [132] uses the difference of two consecutive pixels of an image to classify the difference value of each pair of pixels into a low-level region (pixel difference smaller or equal to 15), middle-level region (pixel difference between 15 and 31), and high-level region (pixel difference greater than 31). The embedding strategy is based on the finding that edge areas can tolerate a larger number of changes compared to smooth areas. In particular, k-bit LSB substitution is used for two consecutive pixels. The value of k depends on the level at which their difference values fall, i.e., a higher level will use a larger value. In [133], an average difference value between the smallest intensity and three additional intensities belonging to a non-overlapping block of 2×2 pixels is calculated and compared with a pre-defined threshold. A block resulting in an average difference value of less than the threshold is classified as a lower-level or smooth block. In contrast, a block having an average difference value higher than the threshold is considered as a higher-level or edge area. In [134], the gradient magnitude of blocks of 3×3 pixels is calculated and then compared with a threshold to classify edge and smooth areas. Many works on this type of LSB data hiding uses edge detectors such as the Canny, Sobel, Fuzzy, Prewitt, and Laplacian of Gaussian edge detector. These edge detectors can be applied individually [135–137] or in a combination as in [138–140]. After classifying a cover image into the edge and smooth areas, their intensities can be used to conceal secret messages such that the pixels belonging to edge areas carry more secret bits compared to pixels in the smooth areas.

Other approaches have focused on embedding secret bits only in the edges of a cover image by varying the edge area to obtain a trade-off between capacity, image quality, and other requirements. In [141], LSBMR is used with an adaptive selection of pairs of pixels. The cover image is divided into non-overlapping blocks of pixels which are rotated by a random degree. A list of pairs of consecutive pixels is collected by raster scanning of each rotated block. The absolute difference between every two adjacent pixels in the list is compared with a given threshold to collect pairs of pixels that are to be used in the embedding process. If the absolute difference is higher than the threshold, the pair of pixels is chosen to hide secret bits. The number of available pairs of pixels is estimated and additional pairs of pixels can be selected by changing the degree of rotation and threshold. Adjusting the threshold value is also done in [142] where the absolute difference value is calculated for 3×3 blocks of pixels of the cover image. Initially, the threshold is set to a high value and the blocks having an absolute difference value higher than the threshold are classified

as edge areas. This algorithm requires the number of edge pixels to be approximately four third of the message length. If this requirement is not fulfilled, the threshold is reduced to obtain a sufficiently large number of edge pixels. In [143], an LSB method is proposed that conceals the secret information in so-called complex regions found by using ant colony optimization (ACO). The size of a complex region is controlled by changing some functions in the classification stages of the ACO algorithm such that it is suitable for the length of the secret message. In [144], the edge pixels are identified using edge detection together with the morphological operation of dilation. Canny edge detection is implemented to detect the edge area and the dilation operation is applied to specify additional pixels nearby the edges. If the capacity for LSB data hiding is not sufficient with respect to the size of the secret message, the threshold of the Canny detection algorithm is adjusted to increase the number of available edge pixels. Furthermore, the size of the structuring element used with the dilation operation to define the number of nearby pixels along the edges can be increased which in turn widens the range of considered surrounding pixels.

Visual Attention-Based: Apart from structural image information, visual attention is a process that condenses the vast amount of visual information arriving at the primary cortex to a small fraction for processing in high-level centers of the HVS. This behavior of the HVS, differentiating among regions of a visual stimulus that are considered as more important compared to other regions, may also be used for advanced LSB data hiding techniques. For example, visual attention models producing saliency maps similar to human perception may be used to advise efficient LSB data hiding solutions and to find suitable locations for data hiding in a cover image.

In [145–147], LSB watermarking schemes are proposed based on the Itti-Koch model [148] for finding pixel-wise saliency maps. A secret message is then embedded into the least salient pixels of the cover image. In [149], a graph-based visual saliency model [150] is applied to a cover image with four-bit planes commencing with the LSB being set to zero. The saliency map is used to distinguish between regions of interest (ROI) and regions of background (ROB). The cover image pixels that fall in the ROB carry up to 4 secret bits while the pixels in the ROI hide less information or none.

A visual saliency model using covariance features [151] is used in [152] to classify ROI and region of non-interest (RONI). In view of applications on resource-constrained devices, in this work, a framework is proposed for combining selective light-weight encryption with LSB steganography. However, some findings reported in [153, 154] suggest that the ROI and RONI should be selected or interacted with by the users, especially, in the fields of medical diagnosis and treatment.

Table 4 summarizes the overall performance of the discussed LSB data hiding techniques in the spatial domain of images. It can be concluded from the reviewed work that LSB replacement offers high capacity while maintaining good visual quality. However, this technique has the drawback that the secret data can be destroyed under noise, data processing, and active attacks. Currently, there exist no studies that find ways to improve the robustness of LSB data hiding in the spatial domain of images except of some reversible LSB data hiding algorithms. The detectability of LSB data hiding in the spatial domain of images can be minimized which comes at the expense of reduced capacity. The security can be strengthened by applying suitable stego-keys and combinations with cryptography algorithms.

3.2. Transform Domain

Discrete Cosine Transform. The DCT is used in many lossy source compression applications such as the Joint Photographic Experts Group (JPEG) format which works with blocks of 8×8 pixels. The data hiding process for source compressed image formats such as the JPEG format is illustrated in Fig. 5. All 8×8 pixel blocks of the raw image are transferred into 8×8 real numbers of the frequency domain using DCT. The obtained real numbers are then quantized using a quantization table to become integer coefficients. The DCT integer coefficients are represented within a given bit width stretching from the MSB to the LSB. Therefore, LSB data hiding techniques can be applied to these DCT coefficients in the frequency domain.

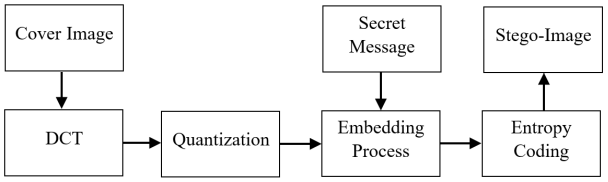

Figure 5. Data hiding in the DCT domain.

Many approaches on LSB data hiding in the DCT domain have similarities to the LSB approaches suggested for the spatial domain. The Jpeg-Jsteg algorithm implementation made available in [155] simply replaces the LSBs of the DCT coefficients by secret bits. The difference to the LSB data hiding in the spatial domain is that the Jpeg-Jsteg algorithm skips all coefficients whose values are equal to zero or one to

Table 4. Performance of LSB data hiding in the spatial domain of images

Reference	Capacity	Imperceptibility	Robustness	Detectability	Security
Conventional LSB data hiding					
[105]	–	–	–	–	–
[106]	4.025 bpp	PSNR = 32 dB	–	–	uses DES and RSA encryption
[107, 108, 110–112]	–	PSNR > 30 dB	–	–	–
[109]	–	PSNR > 55 dB	–	–	–
[113]	–	PSNR > 30 dB	–	–	uses chaotic maps as secret key
[114]	–	PSNR > 30 dB SSIM > 0.98	–	resists RS attack and Chi-square attack	randomizes hiding position with chaotic map
[115]	0.6667 bpp	PSNR = 27.46 dB	–	resists RS attack and Chi-square attack	–
[116, 117]	–	PSNR > 30 dB	–	–	–
[118, 120, 121]	1 bpp	–	–	minimizes number of pixels modified to be undetectable	hiding positions are considered as stego-key
[122–124]	–	–	–	–	applies encryption and hash function for authentication
[125]	1.5 bpp	PSNR > 47 dB	–	passes histogram analysis and Chi-square attack	encrypts secret data using an cryptography algorithm
Reversible LSB data hiding					
[127, 128]	–	PSNR > 30 dB	cover image is recovered	–	uses public/private encryption for data authentication
[129, 130]	1 bpp	PSNR > 45 dB	cover image is recovered	–	–
[131]	1.5 bpp	PSNR > 46 dB SSIM > 0.99	cover image is recovered	resists RS attack and pixel difference histogram analysis	–
HVS based LSB data hiding					
[132, 133]	> 4 bpp	PSNR > 30 dB	–	–	–
[134]	1.49 bpp	PSNR = 44.71 dB	–	–	–
[135–140]	> 3 bpp	PSNR > 30 dB	–	–	–
[143]	> 4 bpp	PSNR > 45 dB	–	–	–
[141, 142, 144]	> 1 bpp	PSNR > 40 dB	–	resists RS attack	–
[145–147]	> 3.8 bpp	PSNR > 40 dB	–	–	–
[149]	–	PSNR > 30 dB	cover image is recovered	–	strong security with large key space against exhaustive search
[152]	–	–	–	–	scrambles secret data using a two-level encryption algorithm
[153, 154]	0.5 bpp	PSNR > 48 dB	–	–	–

avoid confusion in the extraction of the secret bits at the receiver.

In [156], several algorithms such as the F3, F4, and F5 algorithms are described. The F3 algorithm is based on the comparison of the secret bits with the corresponding LSBs of the non-zero value DCT coefficients. In the case that these LSBs match, the LSB of the DCT coefficient is not modified. Otherwise, the absolute value of the DCT coefficient is decreased by one. The F4 algorithm, an amended version of the F3 algorithm, makes the same comparison but distinguishes between negative and positive coefficients with the modification aiming at making the bit-flips occur with roughly the same probability. In [157], additional watermarking processing is performed on the stego-image produced by the F4 algorithm to increase the level of protection of the secret message. The F5 algorithm focuses on scrambling the positions of the DCT coefficients such that the LSB modifications are spread more noise-like over the entire cover image.

Some strategies of LSB data hiding in the spatial domain have also been applied in the DCT domain such as the following. Permutating the DCT coefficients is used in [158] to reduce the detectability of the secret message. Evolutionary algorithms for optimizing secret bit substitution orders to reduce the number of modified pixels in a cover image are used in several approaches such as particle swarm optimization in [159], GA in [160, 161], cohort intelligence and multi random start local search in [162, 163]. The works in [164, 165] applied construction data attachment for the recovery of the cover image in the DCT domain. A combination of LSB data hiding with cryptographic

algorithms in the DCT domain is proposed in [166, 167].

Unlike the pixels in the spatial domain, the DCT coefficients differ from each other in their significance with respect to an image's visual quality. The first DCT coefficient presents the mean of the 64-pixel intensities of a block of 8×8 pixels and is called DC coefficient. The remaining 63 DCT coefficients, referred to as AC coefficients, represent the fluctuation of the pixel intensities in a given block with respect to the mean. The AC coefficients are ordered from less changing (low-frequency) to significantly changing (high-frequency). An LSB modification in high-frequency AC coefficients has little impact on the perceptual image quality compared to an LSB modification in low-frequency AC coefficients. Therefore, the selection of DCT coefficients for LSB data hiding should be adapted based on a trade-off between conserving visual cover image quality and robustness against detecting the secret message. In [168], only DCT coefficients that carry the middle-frequency parts of the cover image are modified using watermark embedding. This algorithm processes between four to sixteen of the 64 DCT coefficients contained in a block during the watermark embedding while the other DCT coefficients are kept unchanged. The algorithm proposed in [169] embeds the secret data in the AC coefficient of the highest frequency. To avoid that the modification in this position is destroyed due to quantization, the values in the quantization table associated with this position is set to one. This results in the AC coefficients not being affected by the quantization processing. In [170], an LSB data hiding method for JPEG-compressed images is proposed that uses all DCT coefficients. A capacity table is derived from the default JPEG quantization table and a simple HVS model in terms of PSNR. In order to avoid distortions to the stego-image, the capacity table is used to estimate the number of bits that can be hidden in each DCT component.

Discrete Wavelet Transform. LSB data hiding approaches have been proposed in the context of one-dimensional discrete wavelet transform (1D-DWT) and two-dimensional DWT (2D-DWT).

1D-DWT: In [171], the integer Haar wavelet transform is used to develop a reversible LSB data hiding technique called difference expansion (DE). This technique transforms pairs (x, y) of pixel intensity values x and y of the cover image into pairs (l, h) of the integer average value l and difference value h of these pixels, i.e.,

$$\begin{aligned} l &= \left\lfloor \frac{x+y}{2} \right\rfloor \\ h &= x - y \end{aligned} \tag{18}$$

Given a secret bit b, the difference value h is expanded as

$$h' = 2 \cdot h + b \tag{19}$$

The expansion of h by b in (19) is equivalent to shifting each bit of the binary representation of h by one position to the left and then appending b as LSB. At the receiver, the secret bit is obtained as the LSB of the difference value h' of the stego-image and the difference value h is recovered as

$$h = \left\lfloor \frac{h'}{2} \right\rfloor \tag{20}$$

The original intensity values x and y of the cover image can be recovered from the respective integer average and difference values using the following inverse transform:

$$\begin{aligned} x &= l + \left\lfloor \frac{h+1}{2} \right\rfloor \\ y &= l - \left\lfloor \frac{h}{2} \right\rfloor \end{aligned} \tag{21}$$

In [172], a generalization of the DE algorithm is proposed which increases capacity and improves computational efficiency. Instead of limiting processing to only two consecutive pixels, the generalized DE uses vectors containing several adjacent pixels of the same color component. A pre-ordering of the pixels placed in each vector can be performed using a security key.

In [173], a block-based DE method is proposed. The cover image is split into non-overlapping fixed-size blocks. These blocks are classified into four complexity levels from Type I to Type IV based on a comparison between the maximum difference value of all pixels in the block with respect to a threshold. While all different values of blocks of Type I are expanded with two secret bits, blocks of Type II and III cover one secret bit using DE and LSB replacement, respectively. Different values of blocks of Type IV do not undergo an expansion. An adaptive segmentation is applied in [174] to improve the capacity and image quality of the block-based DE method. The cover image is divided into pre-defined size blocks larger than two. If the maximum difference between the middle pixel and all other pixels in the block is smaller than the threshold value, each difference value covers two secret bits. Otherwise, the block is broken into four same-size sub-blocks. This classifying and embedding process is repeated until the size of the blocks is equal to two. At this smallest size, the maximum difference is compared with a threshold to decide whether to embed two bits, one bit or to keep the block unchanged.

Apart from the difference value, the prediction error value can be used to design reversible LSB data

hiding. The prediction error expansion (PEE) method is proposed in [175]. In this method, the prediction error values from the neighborhood of a pixel are computed and expanded with secret bits. The PEE method achieves double the capacity and higher image quality compared to the conventional DE scheme. Optimization of the PEE algorithm is described in [176, 177]. The approach is based on the idea of splitting the distortion of the expansion to both the pixel intensity and the predicted intensity. In this way, the impairments caused by modifying the cover image reduce considerably.

Another invertible integer transform is applied in the reversible contrast mapping (RCM) algorithm [178]. Given a grey-scale image of bit depth b, the forward transform of a pair of pixels (x, y) is defined as

$$\begin{aligned} x' &= 2x - y \\ y' &= 2y - x \end{aligned} \tag{22}$$

and the inverse transform is given by

$$\begin{aligned} x &= \left\lceil \frac{2}{3}x' + \frac{1}{3}y' \right\rceil \\ y &= \left\lceil \frac{1}{3}x' + \frac{2}{3}y' \right\rceil \end{aligned} \tag{23}$$

where $\lceil . \rceil$ is the ceil function, $0 \leq 2x - y \leq 2^b - 1$, and $0 \leq 2y - x \leq 2^b - 1$. In the RCM approach, the LSB of the first pixel contains control information and the LSB of the second pixel covers the secret bit. The intensity values of the cover image can be recovered exactly from the stego-image without any additional information. RCM achieves equivalent capacity and image quality but with lower complexity compared to DE and PEE. A generalization of RCM with M-ary modulation is proposed in [179]. Two positive integers are involved in the forward and inverse transform. Any combination of this integer pair can create a different set of transform functions.

2D-DWT: A simple 2D-DWT can be obtained by sequentially performing a horizontal 1D-DWT followed by a vertical 1D-DWT [180]. The 1 level 2D-DWT divides the input signal into 4 groups of DWT coefficients: high-high (HH), high-low (HL), low-high (LH), and low-low (LL). The size of each group is a quarter of the original resolution. The same transform can be applied to the coefficients belonging to the LL subband and be repeated several times to the low-frequency subbands as shown in Fig. 6.

In [181], a reversible image watermarking technique is presented that uses 2D-DWT. The image is divided into non-overlapping blocks which are transformed into DWT coefficients. Depending on the DWT coefficient values in each block, the embedding capacity required by each block is determined adaptively and made available as a matrix. The payload includes the secret message and the side information needed to retrieve the secret message and to reconstruct the cover image. LSB substitution is performed for the payload with the number of secret bits embedded based on the specified matrix.

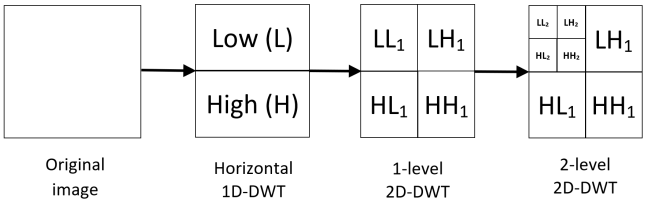

Figure 6. Two-level 2D-DWT obtained by performing horizontal and vertical 1D-DWTs on low-frequency subbands.

A 3D chaotic cat map and an edge-based adaptation are used in [182] to reduce the detectability and perceptibility of LSB data hiding. The individual primary color components of an RGB cover image are transformed by the lifting DWT scheme [183] which will produce approximation coefficients capturing low-frequency information and detail coefficients capturing high-frequency information. The coefficients of each color component are grouped into Set A containing the approximation coefficients and Set D containing the detail coefficients. The 3D chaotic cat map specifies the positions of elements in Set D that are to be used for LSB data hiding. The amount of modification imposed to a detail coefficient of the cover image depends on the smoothness of the region around the related approximation coefficients.

An image authentication and copyright protection method with blind dual watermarking is proposed in [184]. Initially, the RGB color image is converted into YC_bC_r channels. At the first security level, 2D-DWT is performed only on the Y component generating an approximation part LL and three detailed subbands LH, HL, and HH. The LL subband is quantized, embedded with a robust watermark, and the result is used to replace the HH subband. The result is combined with three unchanged subbands to generate a watermarked Y' channel. The Y' channel is then combined with the original C_b and C_r components to construct an RGB color image. At the second level, each primary color component is embedded in a fragile watermark using LSB replacement.

Discrete Fourier Transform. Let an image of size $M \times N$ pixels with pixel intensity at coordinates x and y be denoted as $f(x, y)$ where $x = 0, 1, 2, \ldots, M-1$ and $y = 0, 1, 2, \ldots, N-1$. The discrete Fourier transform (DFT) of the image is defined as

$$F(u, v) = \frac{1}{MN} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x, y) \exp\left\{-j2\pi \left(\frac{ux}{M} + \frac{vy}{N}\right)\right\} \tag{24}$$

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

LSB data hiding may be performed in the real and imaginary parts of the DFT coefficients. In [185], only the real part of the DFT coefficients is used in the design of an LSB-based authentication technique. The cover image is divided into 2×2 blocks which are transformed into the frequency domain. The real parts of three out of four DFT coefficients in each block are chosen to cover secret bits using LSB replacement. The inverse DFT is then applied to transform the pixel intensities back to the spatial domain.

In [186], both the real and imaginary part of the coefficients obtained from DFT-transformed 2×2 blocks are used for LSB data hiding. The LSBs of three bytes excluding the first byte of each DFT-transformed 2×2 block of the cover image are substituted. The embedded blocks are transformed back into spatial domain and processed by GA to enhance security.

In [187] the multiple parameter discrete fractional Fourier transform (MPDFRFT) is used to generate frequency coefficients. In each transformed 8×8 block, 8 decimal coefficients are selected randomly, converted to binary form, and then embedded with secret data. Furthermore, this work is improved using two-dimensional MPDFRFT and random discrete fractional Fourier transform algorithms before applying the LSB technique.

Table 5 summarizes the performance of the discussed LSB data hiding techniques in the transform domain of images. Compared to the spatial domain, given acceptable visual quality, the capacity of LSB data hiding in the transform domain is considerably lower than in the spatial domain of images. On the other hand, it achieves a higher level of robustness such that secret data can resist a variety of impairments such as noise, data processing, and active attacks. Due to the high robustness, LSB data hiding in the transform domain is used in many strong watermarking techniques. Although LSB data hiding in the transform domain can resist advanced steganalysis and supports strong confidentiality with encryption, there are only a few studies that take detectability and security into account.

3.3. Quantum Domain

With the recent advances in quantum computing, applications such as quantum image processing have also emerged. An image can be expressed in quantum bits, so-called qubits, which are used to express a quantum image in the flexible representation of quantum image format (FRQI) [189] and the novel enhanced quantum representation of digital images format (NEQR) [190]. Because it is easier to transform a conventional image into a quantum image using the NEQR format, research on LSB data hiding in the quantum domain has been focusing on this format.

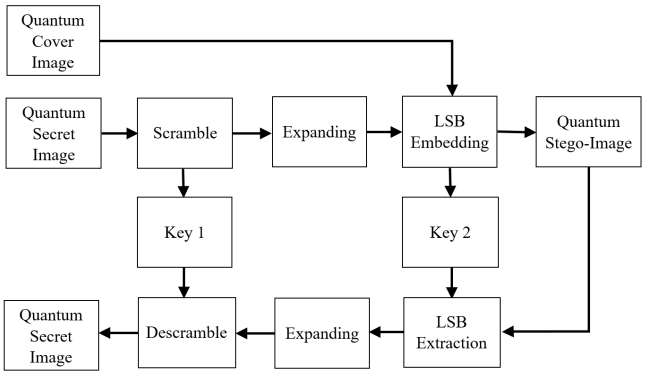

Figure 7. LSB data hiding in the quantum domain (see also [192]).

An NEQR-based quantum image can be expressed as

$$|I\rangle = \frac{1}{2^n} \sum_{i=0}^{2^{2n}-1} |c_i\rangle \otimes |i\rangle \tag{25}$$

where $|c_i\rangle = |c_i^{q-1}, \ldots, c_i^1, c_i^0\rangle$; $c_i^k \in \{0,1\}$; $k = q-1, \ldots, 1, 0$ encodes the gray-scale intensity of a pixel. Further, c_i^0 is the lowest qubit of $|c_i\rangle$ or the LSB in the quantum domain. The operator $\otimes$ denotes the Kronecker product. The location information $|i\rangle$ with $i = 0, 1, ..., 2^{2n} - 1$ can be organized into vertical and horizontal coordinates as

$$|i\rangle = |y\rangle|x\rangle = |y_{n-1}y_{n-2}...y_0\rangle|x_{n-1}x_{n-2}...x_0\rangle \tag{26}$$

where $|y_j\rangle|x_j\rangle \in \{0,1\}$. The following two blind LSB steganograpy algorithms for quantum images in the NEQR format are proposed in [191]. The plain LSB method substitutes a least significant qubit c_i^0 of $|I\rangle$ of the cover quantum image by a secret qubit of the secret quantum message. The block LSB approach splits the cover quantum image into blocks, scrambles the pixel positions, and hides one message bit in each pixel intensity.

A general model of LSB replacement in the quantum domain is illustrated in Fig. 7. As a prerequisite, the conventional spatial pixel-based format of the cover and secret image is converted into the NEQR format of the quantum domain. Because the size of a cover image is often a multiple of the size of a secret image, the LSB replacement is done like an injection function to mimic two same-size sets. The quantum secret image is then scrambled to secure its content, e.g., using Arnold scrambling [193], Hilbert scrambling [194], SWAP gates [195], or rotation of qubits [196]. The embedding and extraction of the secret quantum image may be performed using an XOR operation or be controlled by pre-defined keys [192, 197, 198].

Other aspects of LSB data hiding such as security, quality, and robustness have also been studied in the

Table 5. Performance of LSB data hiding in the transform domain of images

Reference	Capacity	Imperceptibility	Robustness	Detectability	Security
[156]	0.134 bpp	–	–	–	–
[157]	–	PSNR > 40 dB	–	–	–
[158]	> 0.14 bpp	PSNR > 30 dB	–	resists tests related to Chi-square attack and S-family attacks [188]	–
[159]	1.125 bpc	PSNR > 30 dB	–	–	–
[160]	0.0625 bpc	PSNR > 54 dB	–	–	–
[161]	2 bpc	PSNR > 40 dB	robust against salt and pepper noise, Gaussian noise, median filter	–	–
[162, 163]	1.125 bpc	PSNR > 29 dB	–	–	–
[164]	0.117 bpp	PSNR > 35 dB		–	–
[165]	0,015625 bpc	PSNR > 40 dB	–	–	–
[166]	–	PSNR > 20 dB	partly robust against salt and pepper noise	–	secret data is encrypted before being embedded
[167]	1 bpc	PSNR > 60 dB	–	–	secret data is encrypted using AES algorithm
[168]	0.25 bpc	PSNR > 40 dB	–	–	–
[169]	0,015625 bpc	PSNR > 38 dB	strong against JPEG compression	–	–
[170]	–	PSNR > 35 dB	strong against JPEG compression	–	–
[171]	1.97 bpp	PSNR > 16 dB	cover object is recovered	–	–
[172]	–	PSNR > 20 dB	cover object is recovered	–	–
[173]	0.48 – 1.18 bpp	PSNR > 34 dB	cover object is recovered	–	–
[174]	1.3 bpp	PSNR > 30 dB	cover object is recovered	–	–
[175]	–	PSNR > 30 dB	reversible watermarking	–	–
[176, 177]	–	PSNR > 20 dB	reversible watermarking	–	–
[178]	–	PSNR > 15 dB	reversible watermarking	–	–
[179]	–	–	robust against Gaussian noise and median filter	–	–
[181]	–	PSNR > 25 dB	reversible watermarking	–	–
[182]	2.25 bpp	PSNR > 45 dB SSIM > 0.998	–	passes visual attacks, image histogram, similarity measures	a chaotic map is used as stego key
[184]	0.4 bpp	PSNR > 29 dB SSIM > 0.94	provides both fragile and robust watermarks	–	–
[185]	–	–	–	against Chi-square attack and histogram analysis	–
[186]	–	PSNR > 40 dB	–	–	–
[187]	–	PSNR > 50 dB	robust against certain attacks[1]	–	–

[1] Compression, Gaussian noise, speckle noise, salt and pepper noise, filtering, rotation, and colour tone attacks

quantum domain. In [194, 199], the reflected binary code, also known as Gray code, is used to encode qubit segments belonging to the secret message. In [200], a two-level LSB data hiding method is proposed. A secret image is encrypted and embedded into a quantum watermark image using the modified LSB data hiding method. Then, the watermarked image is hidden in the quantum cover image using the same data hiding method. This approach offers strong security through two-level LSB data hiding and encryption of the secret image.

Regarding image quality, the edge region of the quantum cover image is used for data hiding in [201]. In particular, watermarking information is embedded in the edge regions of the quantum cover image using linear LSB data hiding. In [202], the LSB substitution is combined with the neighbor mean interpolation (NMI) method in the quantum domain. The quantum cover image is enlarged by the NMI algorithm and divided into blocks of 2×2 qubits. In each block, the watermark image qubits are embedded into the LSBs of three out of four pixels of the quantum cover image. This method considerably reduces the distortion and blur of image texture caused by LSB modification.

In [203], the PVD method is used for adaptive LSB data hiding. In this approach, quantum circuits are used to calculate the PVDs of three pairs of pixels in each of the 2×2 blocks of the quantum cover image. The respective blocks are classified into lower level (or smooth) and higher level (or edge) blocks depending

in which of six ranges the obtained PVD falls, i.e., R1=[0, 7], R2=[8, 15], R3=[16, 31], R4=[32, 63], R5=[64, 127], and R6=[128, 255]. The lower level consists of R1 and R2, the higher level includes the remaining four ranges. Then, 4-bit LSB replacement is applied in the edge block, while only 3 LSBs are replaced in smooth blocks. This approach achieves good visual quality, strong robustness against noise, and offers high security.

Table 6 provides a summary of the performance of the discussed LSB data hiding techniques in the quantum domain of images. It should be mentioned that current work has limited scope focusing on spatial LSB replacement in the context of qubits. Although the research on LSB data hiding approaches in the quantum domain has been published rather late compared to the other domains, their performance assessment is more comprehensive with often four among five attributes being considered. Overall, the proposed approaches not only offer high capacity with good visual image quality, but also provide good security by scrambling secret bits and hiding positions. However, robustness against common noise conditions such as salt and pepper noise has been observed as being rather poor while almost all works used histogram steganalysis to detect stego-images. Given further advances in quantum technology during the coming years, new formats and processing operations for digital media in the quantum domain can be expected which may offer more opportunities for LSB data hiding in the quantum domain.

3.4. Applications

In this section, applications of LSB data hiding in images are presented. A well-known application is the protection of copyrights of images. Information related to the image such as ownership is embedded as a watermark used to verify the authenticity of the cover image among others and to trace copyright infringements. However, LSB data hiding has been applied to many other fields such as medical and health care systems, social networks, IoT, and telecommunication systems.

Protection of Copyrights: In [204], the face template of people is covered inside a biometric image to ensure the matching between identity and respective biometric data. Similarly, in [205], the handwritten signature is concealed in a biometric watermarking image for copyright protection.

Medical and Health Care Systems: An e-medicine system is proposed in [206], which hides the password and biometric parameters into the image of the card owner. The obtained stego-image and other information such as symptoms of the patient and treatments performed by the medical doctor are stored and updated in a smart card. Therefore, instead of bringing many documents, patients only carry a small card that can be used anywhere in the e-medicine system. In [207], two LSB algorithms are proposed to secure data of the patient using the standard of digital imaging and communication in medicine (DICOM). All individual information of a patient, doctor's diagnosis and treatment, and an electroencephalogram image are embedded into a magnetic resonance image which is a part of the DICOM payload. In [208], the transmission of key frames during wireless capsule endoscopy is protected by a combination of LSB data hiding and a three-level encryption algorithm. Other applications of data hiding in medical and health care systems can be found in [209].

Internet of Things: Because LSB data hiding is simple and computationally inexpensive, it is suitable for use in resource-constrained IoT devices. In [210], LSB data hiding is used to hide encrypted sensor data, MD5 digest, and encryption key in a cover image that is transmitted from an IoT device to the home server. Furthermore, the data transfer between the home server and the cloud is also protected by a combination of LSB data hiding and AES algorithm. In [211], LSB data hiding solves the key distribution problem of cancelable iris biometric systems. To set up the control right of a remote surveillance IoT network, the iris feature of the administrator is collected and transformed by a one-way function with a user-specific key. The key is hidden in a cover image and separately updated on the IoT server with the feature data. In the case that the user needs to access smart objects, the user key is extracted from the stego-image. The transformed feature data is calculated once again with the extracted user key and newly captured iris data. The legitimate user is identified by a matching process between old and new feature data. In [212], an LSB-based hybrid pixel indicator technique is implemented on a 32-bit controller. The cover image is divided into non-overlapping groups of three consecutive pixels. The LSBs of the first pixel are used as indicator bits showing the number of bits to be embedded in the LSBs of the other pixels of the group.

Social Networks: Although online social networks are widely used for sharing of images, there is a lack of privacy and copyright restrictions on them. Images from the web can be downloaded, modified, and uploaded in other places without considering the copyright of the data. The lack of privacy, integrity, and authenticity of visual content is a problem that needs to be resolved. In [213], a solution to this problem is proposed. An input image is scrambled with a key to protect the privacy of image content while a secret image is encrypted by an iterative magic matrix-based encryption algorithm. The encrypted secret image is substituted into the Y-component of the scrambled image in the YC_rC_b color model format by an adaptive LSB data hiding method. The embedded Y-plane is

Table 6. Performance of LSB data hiding in the quantum domain of images

Reference	Capacity	Imperceptibility	Robustness	Detectability	Security
[191]	–	PSNR > 49.9 dB	each secret bit is embedded several times for self-recovery	scrambles secret bits to enhance undetectability	–
[193]	–	PSNR > 54 dB	–	–	secret bits are scrambled to enhance the confidentiality
[194]	4 bpp	PSNR > 47 dB	robust against salt and pepper, qubit flip noise, fragile for Gaussian noise	makes a slight jitter under histogram analysis	secret bits are scrambled to enhance the confidentiality
[195]	–	PSNR > 43 dB	reduces effect of salt and pepper noise	–	secret bits are scrambled to enhance the confidentiality
[196]	–	PSNR > 51 dB SSIM > 0.97	acceptable robustness under quantum channel noise	–	secret bits are scrambled to enhance the confidentiality
[192]	–	PSNR > 54 dB	–	passes histogram analysis	secret bits are scrambled to enhance the confidentiality
[197]	2 bpp	PSNR > 57 dB	adapts well to salt and pepper noise and brightness changes	–	secret bits are scrambled to enhance the confidentiality
[198]	0.5 bpp	PSNR > 50 dB	–	–	secret bits are scrambled to enhance the confidentiality
[199]	2 bpp	PSNR > 55 dB	resists noisy environments	passes histogram analysis	secret bits are scrambled to enhance the confidentiality
[200]	2 bpp	PSNR > 48 dB	robust under salt and pepper noise	–	uses two-level embedding scheme, encrypts secret data
[201]	0.25 bpp	PSNR > 57 dB	–	passes histogram analysis	–
[202]	–	PSNR > 54 dB	fragile watermark helping to detect the attacks easily	–	secret bits are scrambled to enhance the confidentiality
[203]	–	PSNR > 39 dB	robust under salt and pepper noise, secret data is recovered by adding the parity bits	resists the RS attack	–

then combined with the two other color components and converted to an RGB stego-image. Similar work to secure visual contents in social networks is reported in [214] where the secret image is encrypted by a three-level encryption algorithm. The Morton scanning directed LSB technique is used to hide secret blocks into the I-component of the cover image in the hue, saturation, intensity color model format.

Telecommunication Systems: Reversible watermarking is used in [215] for transmission of satellite imagery. The description information of all blocks of the cover image is considered as a watermark that is embedded into different blocks of the cover image. At the receiver, a recovery process is performed to retrieve the original satellite cover image. In [216], an LSB data hiding technique is used to verify the sources of photographs captured by an unmanned aerial vehicle. Furthermore, LSB data hiding is combined with cryptography in applications such as the electronic voting system [217] [218] or the ATM transaction [219].

Others: Some other applications using LSB data hiding in mobile devices and computers are SmartSteg and OTP-Steg, respectively:

- SmartSteg [220]: The SmartSteg software, designed for Android mobile devices, allows transmitting secret information between Android smartphones.
- One-time Pad Steganography [221]: The one-time pad steganography (OTP-Steg) is an LSB data hiding software running on computers. It contains three functions, i.e., generating OTP keys, encryption including LSB embedding, and decryption along with extracting data from the stego-image. OTP-Steg can process images in png and BMP format. The OTP-Steg software tool and related documentation can be found in [222].

4. LSB Data Hiding in Videos

In this section, a review of LSB data hiding methods for videos is provided with respect to the classification shown in Fig. 2. Accordingly, LSB data hiding in images may be classified into raw data and compressed data methods.

4.1. Raw Data

A raw video such as an audio-video interleaved (AVI) file is a sequence of same resolution frames in which each frame is considered as an independent color image. Thus, LSB data hiding techniques developed for images can be applied to a single, several, or all frames of a cover video. The difference to LSB data hiding in images is that the sequence of frames is arranged temporally in a specific order. Therefore, the temporal factor, frame order, and the relationship between frame content need to be taken into account. The following sections

will provide a review of image-based LSB data hiding techniques for videos, LSB authentication algorithms for videos, and object-based LSB data hiding methods.

Image-based LSB Data Hiding. LSB data hiding in the spatial domain has been dominating the image-based LSB data hiding approaches for videos. In [223], a self-recovery video authentication watermarking approach is introduced which applies the reversible LSB data hiding described in Section 3.1. This approach operates on blocks associated with some selected keyframes. The authentication and recovery data is calculated and attached to form a watermark for each block. Each block covers its own watermark with LSB modification as described in [122].

Many image-based LSB approaches for videos are carried out independently and equally to every cover frame and color component of the cover video. In [224], a secret message is divided into several same-size blocks which are embedded consecutively into the sequence of cover frames of the cover video. Every LSB and second LSB of the selected pixels of the three primary color components of a cover frame are replaced by the secret bits. The length and format of the secret message are varied and the secret bits of each block are permuted randomly to improve security. The algorithm proposed in [225] also replaces the LSB and second LSB of pixel intensities of every cover frame by the bits of an encrypted message. The number of frames used in the embedding process is selected randomly among all frames of the cover video in AVI format. The positions of pixels are chosen randomly by the knight tour algorithm [226] to strengthen security.

Regarding the number of secret bits to be hidden in a cover video, some works take account of the HVS being more sensitive to changes in some color components than to changes in other color components. In [227], a 3-3-2 LSB data hiding method is proposed for covering secret bits which uses three bit planes of the red and green color component while only the LSB and second LSB of the blue color component are used. This approach is based on the fact that the HVS is more sensitive to changes in blue color than in red and green color. In [228], another 3-3-2 LSB data hiding method is suggested for hiding secret messages in a cover video. In this method, the visual quality of the stego-frames is optimized with respect to the MSE and HVS deviation quantified by SSIM before these stego-frames are merged with non-modified video frames. In [229], LSB data hiding is applied to the YUV color space of the uncompressed cover frames. The secret bits are embedded into the three lowest bit planes of the Y component and the two lowest bit planes of the U and V component. In particular, to strengthen security, the pixels of the YUV components of the cover frames and the data of the secret message (one-dimensional representation of a binary image) are first scrambled by a key that is shared between sender and receiver. A $(7, 4)$ Hamming code is used to protect each group of $k = 4$ bits of the secret message against errors. The encoded secret message is then XORed with random values using a private key. The result is embedded in the scrambled pixels of the YUV components of the cover video frames to form stego-video frames. Finally, the pixels of the stego-video frames are rearranged to the original pixel positions of the cover frames.

LSB data hiding techniques for images in the transform domain have also been applied to hide secret messages in cover video frames. In [230], the frames of a cover video in AVI format are divided into four equal parts and each byte of a secret image in BMP format is also split into four pairs of bits. The DCT image steganography method proposed in [231] is then applied to hide each pair of secret bits into the respective quadrants of the cover frames. In [232], a video steganography algorithm is proposed based on LSB substitution of integer wavelet coefficients. The RGB components of the cover frames are divided into blocks of 8×8 pixels which then undergo an integer Haar wavelet transform (IHWT). The embedding of the secret messages uses only the middle and high-frequency subbands of the IHWT coefficients, i.e., HL, LH, and HH frequencies, in order to provide a trade-off between high capacity and good video quality. Similarly, IHWT is applied to the Y, U, and V components of the cover frames in [233]. A secret message is encoded using a BCH (15,11) code to improve the reliability of the algorithm. The encoded secret message is XORed with a sequence of random numbers produced by a key. The result is embedded into the HL, LH, and HH frequencies of the cover frames giving stego-video frames.

Video Authorization. In view of the large number of frames involved in composing a video, it is more challenging to conserve integrity for videos than for images. Video frames can be attacked easily by removing, inserting, and tampering frames or forging video watermarks with common editing video software. Therefore, considering and processing each video frame as an independent image may not be sufficient to protect video content. It is necessary to not only verify the integrity of each individual video frame but also to consider the relationship between video frames.

In [234], the concept of a frame-pair is introduced to provide protection against video tampering. In particular, the cover video is divided into segments including several frames where each frame of a segment is paired with a frame from an adjacent segment. Then, the first frame is re-quantized from 24-bit to 3-bit color whose RGB components are encrypted and embedded into respective components of the second frame. In this

way, the watermark is dynamic and depends on the content of the first frame which makes it harder to tamper with. This frame-level authorization can detect replacement, insertion, and corruption. In case that one frame is damaged, it can be recovered by the watermark extracted from the subsequent frame. In [235], two block-level authorization algorithms, called VW16E and VW8F, are described which work with 2×2 blocks of four consecutive 16-bit pixels. The cover pixels can come from the same or different video frames and include 8 MSBs and 8 LSBs. The integrity bits, generated from the MSBs of pixels and the block address, are combined with the confidential bits that are provided by a text file to form the watermark. In VM16E, a 16-bit watermark replaces 4 LSBs of each pixel while an 8-bit watermark of VM8F substitutes only two LSBs. In [236], two-level LSB watermarking is suggested to improve the accuracy of detecting and localizing video tamper. The cover video is divided into temporal and spatial sub-blocks. For each type of sub-block, a new non-negative matrix factorization calculates their sparseness constraints which are considered as block descriptions. The block signature is generated from six MSB planes of each sub-block. The block description and signature of each sub-block are merged, encrypted, and embedded into the second LSB and the LSB of the intensities of that sub-block. This technique is useful for not only authorization purposes but also recovery of tampered areas of the cover video.

The above methods may run into efficiency problems when the number of frames becomes very large which in turn induces a high computational load. Instead of applying authentication related processing to all cover frames, a solution is to modify several groups of frames. The algorithm in [237] operates on a number of non-overlapping packages of frames, referred to as windows. In each window of frames, a keyframe is chosen as a center frame in the key segment of a certain length. A JPEG compressed version of the keyframe is used as reference information for both authorization and recovery. This reference information is split into many symbols which are combined with their hash values to form the watermarks embedded in all blocks of cover frames in the segment. The frame which is not in the segment can cover the index information of that frame.

Object-based LSB Data Hiding. In the raw format, the frames of a video with the same scene usually differ in moving objects. Several works in watermarking and steganography have therefore focused on processing regions where objects move. In [238], a dual watermarking method is presented that uses the region of moving objects. For each video frame, the extraction of the moving object regions is performed with reference to synthesized background frames. The index of the current frame is considered as the first watermark which is embedded into moving object areas using the DE algorithm [171]. The second watermark is calculated from the MSBs of a frame and the LSBs of the moving objects which are covered by the reversible LSB data hiding technique presented in [239]. This authentication method can protect video content from spatio-temporal tampering, and recover the modified regions and moving objects. In [240], a video steganography algorithm uses motion-based multiple object tracking to identify ROIs. A Gaussian mixture model is combined with morphological operations to subtract the background and identify object regions. Kalman filtering is performed to estimate the object trajectory. The encrypted secret message is concealed in the two lowest bit planes of the RGB color components of the pixels in areas containing objects. The keys used in the encryption process are also hidden in the non-motion area of the first cover frame and transmitted secretly to the receiver. This LSB steganography algorithm is improved in [241] by combining two face detectors for the case that the objects are human faces. The most powerful and fast object detection algorithm, called Viola-Jones, is applied for the first frame and the Kanade-Lucas-Tomasi algorithm is used for the remaining cover frames. This method gives good accuracy of face detection while it reduces the computational load associated with the detection process. An extension of this work into the transform domain is reported in [242]. The moving object regions in the cover frames are extracted and the intensities falling in these regions are transformed into frequency coefficients. The processed secret message is hidden in the LL, HL, LH, and HH subbands obtained by 2D-DWT or the DC/AC coefficients obtained by 2D-DCT. The stego-regions in the transform domain are converted back to the spatial domain by an inversion transform and combined with respective non-motion regions to rebuild stego-frames.

Table 7 summarizes the performance of the discussed LSB data hiding techniques in the raw domain of videos. Similar to the spatial domain of images, LSB data hiding in the raw domain of videos provides large capacity while maintaining good visual quality. Regarding robustness, LSB data hiding techniques in the raw domain can, to some extent, resist noise and filtering attacks while the secret data and cover object can be recovered. Because almost all works are applied to watermarking applications, their focus is on detecting and accessing easily and effectively the watermark rather than concealing its existence. In addition, encryption is used to achieve stronger confidentiality and integrity of the watermarking algorithms.

Table 7. Performance of LSB data hiding in the raw domain of videos

Reference	Capacity	Imperceptibility	Robustness	Detectability	Security
[223]	–	PSNR > 23 dB	cover object is recovered using hidden data	be detected easily to prevent temporal and spatial tamper	–
[224]	–	PSNR > 50 dB	–	–	–
[225]	–	PSNR > 59.9 dB	–	–	encrypts secret message and randomizes hiding position
[227]	2.667 bpp/frame	–	–	–	–
[228]	2.667 bpp/frame	PSNR > 32 dB	–	–	–
[229]	2.333 bpp/frame	PSNR > 51 dB	corrects errors using a Hamming code	–	hiding position is scrambled by three shared keys
[230]	–	PSNR > 46 dB	–	–	each byte of secret image is segregated randomly into four quadrants
[232]	–	–	–	passes histogram analysis	–
[233]	1.125 bpp/frame	PSNR > 34 dB	robust under median filter attack, corrects errors using BCH (15, 11)	–	encrypts secret message
[234]	–	–	lost frames are recovered using hidden data	–	indices of frame-pairs are considered as stego-key
[235]	–	VW16E: PSNR > 34 dB VW8F: PSNR > 47 dB	–	watermark can be detected easily to prevent tamper	–
[236]	–	PSNR > 33 dB	cover frames under spatial tampering and frame deletion can be recovered	watermark can be detected easily to prevent spatial and temporal tamper	hash function and encryption algorithm are applied
[237]	1 bpp/frame	PSNR > 47 dB SSIM > 0.99	reconstructs well video content if tampering rate ≤ 67%	watermark can be detected easily to prevent inter- and intra-frame tamper	hash function is used to generate the watermark
[238]	–	PSNR > 37 dB	supports recovering tampered regions and the moving objects of video frames	watermark can be detected easily to prevent spatial and/or temporal tamper	–
[240]	–	PSNR > 40 dB	–	–	encrypts secret message
[241]	embedding ratio = 5.5 % to 21.9 %	PSNR > 33 dB	robust under certain attacks[1], corrects errors using a Hamming code	–	encrypts secret message
[242]	data hiding ratio ≈ 3.4 %	PSNR > 48 dB	robust under certain attacks[1], corrects errors using Hamming and BCH codes	–	encrypts secret message

[1] Salt and pepper noise, Gaussian white noise, and median filtering attacks

4.2. Compressed Domain

Video compression is more complicated than image compression. It includes intra-frame compression, inter-frame compression, and lossless entropy coding as illustrated in Fig 8. While intra-frame compression is performed individually and independently on each video frame, inter-frame compression considers both spatial and temporal relationships between two or more video frames.

Frame Compression. ***Intra-frame Compression:*** In intra-frame compression, each video frame is considered as an image and compressed using either DCT or DWT. In [245], LSB data hiding is applied to a video conference system using the H.261 video compression standard. The video frames are classified into I-frames containing independent values of brightness and P-frames carrying values of motion estimation and compensation. Each block of 8×8 pixels is transformed into a block of 8×8 DCT coefficients. LSB replacement is performed on blocks that have at least one DCT coefficient greater or equal to a predefined value. It should be mentioned that the motion vector may be affected by the LSB modification. Similarly, LSB modification is performed on the non-zero DCT coefficients in all I-, P-, and B-frames of MPEG-2 videos in [246]. In [247], a watermarking scheme for high-efficiency video coding (HEVC) is proposed that conceals one secret bit in the LSB of each quantized transform coefficient (QTC).

Combination of Intra- and Inter-frames: The LSB data hiding techniques with purely intra-frame compression are implemented right before the step of entropy coding. The embedding process has no impact on inter-frame compression because the DCT coefficients used for block reconstruction remain unmodified. However, two problems of this approach are addressed in [248], i.e., mismatch of watermarked

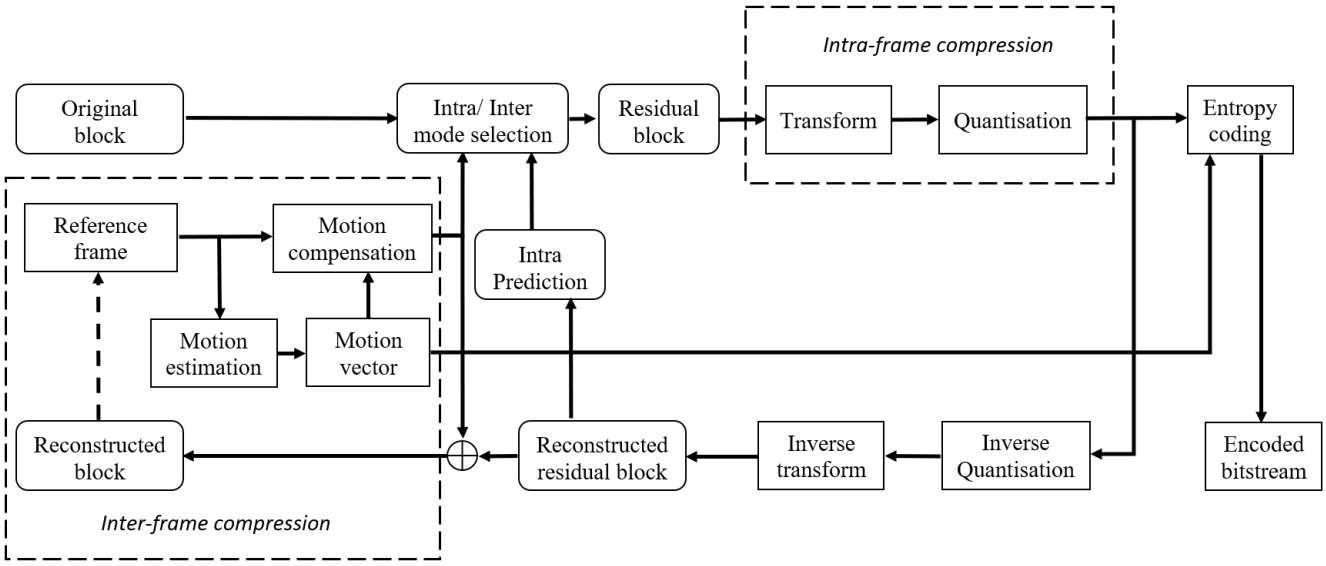

Figure 8. Flow process of video compression (see also [243, 244]).

blocks at the decoder and rate-distortion. In particular, an LSB watermarking technique is proposed that considers both intra- and inter-frame compression. The embedding process is still performed on QTCs. For the use of n bit planes, the magnitude of selected QTCs is required to be greater than the threshold of $2^n - 1$. The output blocks of the intra-frame compression are used as the input blocks of the inter-frame compression. The residual blocks are reconstructed from the watermarked DCT coefficients and all the motion estimation and compensation are affected by LSB modification. An optimization of rate distortion is used to select the best prediction mode for mitigating negative effects of the embedding process on video quality and the bit rate produced by the rate distortion bit allocation algorithm.

Intra-prediction Mode: In advanced video compressions such as H.264 and H.265 (HEVC), the prediction is not limited to the temporal relationship between subsequent frames but also exploits spatial redundancy in terms of correlation among pixels within a given frame. The planar prediction mode supports all block sizes defined in HEVC and is not restricted to a block size of 16×16 pixels as in H.264/MPEG-4 AVC. The correlation between blocks of pixels of the same frame can be predicted by an intra-frame prediction process. The blocks of pixels in the intra-prediction mode vary in size and contain luminance samples within several modes which can serve as cover space for LSB data hiding. In [249], a high capacity data hiding algorithm using the intra-prediction mode (IPM) for videos in H.264/AVC format is presented. The H.264/AVC standard includes 4 types of modes: Intra 4×4, Intra 16×16, Intra chroma, and intra pulse code modulation (IPCM). The Intra 4×4 mode is the most suitable for LSB data hiding because it encodes significant details of the frame. In this mode, each 16×16 pixel macroblock is divided into 16 4×4 pixel sub-blocks comprising 4 luminance samples, DC prediction mode, and 8 directional prediction modes. A number of sub-blocks are chosen as candidate-hiding blocks. With each sub-block containing 9 IPMs, the best IPM is chosen, which has the least Lagrangian cost. If the LSB of the best IPM equals the secret bit, then modification is not performed. Otherwise, an alternative IPM will be used to cover the secret bit. The alternative IPM has a different LSB than the best IPM and has the least Lagrangian cost among the remaining modes. Because this LSB modification is based on the Lagrangian cost and uses an adjustable number of 4×4 luminance sub-blocks, video quality degradation is minimized and adjusted. In [250], an LSB data hiding on IPM is combined with encryption to secure the scalable video coding (SVC). This approach also processes 4×4 sub-blocks containing nine 4-bit IPMs. An algorithm is presented that chooses pairs of continuous IPMs such that the LSB modification on these IPMs causes the least distortion. Then, the LSBMR technique is performed on the selected pair of IPMs. In [243], a matrix coding-based data hiding technique is used on the 4×4 IPMs of HEVC videos. The LSBs of the IPMs are not modified directly but used to set the mapping rules between k secret bits and a group of n IPMs. The position of the element which needs to be modified is calculated from the k secret bits and the n LSBs of the IPMs. If the position is zero, no IPM is modified. Otherwise, the IPM having the position equal to that value is changed to map the secret information and minimize the rate distortion.

Motion Vector. A motion vector is an essential element in motion estimation (ME) and compensation which constitute the main steps of inter-frame compression. It represents a macroblock in a frame based on the location of this macroblock in a reference frame. A motion vector can be represented by horizontal and vertical components, or magnitude and phase angle. It is paired with a prediction error showing the accuracy of the associated macroblock reconstruction. The attributes of a motion vector such as magnitude and phase offer a potential space for LSB data hiding.

Motion Vector Attributes: Depending on the magnitude and phase angle associated with a motion vector, LSB replacement is performed in the horizontal and vertical component representation of the motion vector in [251]. The motion vectors having magnitude higher than a threshold are used in the embedding process. The phase angle is considered as a classifier to choose the cover objects. If the phase angle is acute (less than 90°), LSB replacement is applied to the horizontal component of a cover object. If the phase angle is obtuse (between 90° and 180°), LSB replacement is performed in the vertical component. If the phase angle is equal to 45°, both components are used as a cover environment. In [252], both the horizontal and vertical components of motion vectors in each P- and B-frame are used in the embedding process. However, instead of using the magnitude for identifying eligible motion vectors, the selection of motion vectors is based on the associated prediction error. The rationale behind this approach is that the motion vector does not represent the true motion but predicts the moving of macroblocks. A modification of a motion vector with high prediction error has a lower effect on the reconstruction quality. Therefore, this approach selects those motion vectors that have a prediction error higher than a threshold and embeds the secret bits sequentially in the horizontal and vertical components. The prediction errors associated with modified motion vectors are also varied for each frame and hidden in I-frames.

Motion Vector Estimation: Unlike the motion vector attribute approaches, which process the actual motion vectors, some LSB data hiding techniques modify the motion vectors during the estimation process. In [253], the uncertainty associated with ME is exploited for information hiding to improve the undetectability of secret messages. This algorithm is based on the fact that ME executed with different parameters may output different motion vector values for the same block. First, ME is performed to calculate motion vector values and its uncertainty presented via the expected sum of absolute difference (SAD) between blocks. All the LSBs of horizontal and vertical components of all motion vectors are collected to form a so-called binary channel. The embedding process uses an STC [55] to convert this binary channel into a list of secret bits with minimum impact on video quality. If the LSBs before and after encoding are the same, the motion vector value is kept unchanged. Otherwise, a full search of possible motion vector values is conducted to find a new motion vector value among all possible ones which have the same LSB and minimum SAD. Finally, the compressed frame is constructed with modified motion vectors that have the highest acceptable uncertainty. The search for a suitable motion vector used in the LSB replacement is improved in [244]. This algorithm is called motion vector modification with preserved local optimality and achieves a higher security level compared to conventional motion vector-based steganographic methods. By adjusting the embedding operation to minimize distortion, a two-layered STC method is applied to LSBs of one among two motion vector components with given distortions in [254]. The distortion is calculated based on the statistical distribution change of motion vectors and the prediction error change caused by modifying the motion vectors.

Entropy Coding. Because entropy coding aims to reduce the redundancy in presenting the DCT coefficients after frame compression, the available space for LSB modification in entropy codes is limited. Several LSB techniques have been proposed for context-based adaptive variable length coding (CAVLC) and context-based adaptive binary arithmetic coding (CABAC) to protect the authentication of video streams.

The CAVLC method explodes the fact that many AC coefficients are zero. It reorders the DCT coefficients belonging to a block in a zig-zag scan and represents them in tuples of their values and the number of zeros preceding those coefficients. These tuples are encoded by variable length codes (VLCs) and each block is terminated by an end of block (EOB) mark. In [255], real-time labeling LSB data hiding for MPEG-2 compressed videos is proposed. This approach uses the fact that LSBs of suitable VLCs which have the same run length, differ one value in level, and are equal in codeword length. This condition ensures that the LSB modification causes invisible quality degradation and keeps the size of the video stream the same. VLCs of AC coefficients of intra- and inter-frames can be used for data hiding while the DC coefficients cannot be used. During the embedding process, an lc-VLC is selected such that changes in the VLC cause perceptual invisible degradation and the original size of the MPEG bitstream are kept the same. If the LSB of a selected lc-VLC equals the secret bit, LSB replacement is not performed. Otherwise, the VLC is replaced by another VLC whose LSB-level represents the secret bit.

The CABAC approach uses the information of the previously encoded blocks to predict and encode the current block, i.e., all blocks are encoded in

context. Its efficiency is higher but processing is more complicated than CAVLC consisting of three steps: Context modeling, binarization, and arithmetic coding. For each 4×4 block, several parameters that characterize the context of the block are calculated. The so-called coded block pattern (CBP) determines the context of the current block from neighboring blocks. The higher the CBP value is, the more significant coefficients are contained in that block. The significant coefficient map (SM) shows the position of coefficients having the absolute value equal to or larger than one. The level information (LI) presents the levels of the coefficient from one to nine through a reverse zig-zag scanning of that 4×4 block. In [256], a watermarking method is proposed using the coefficients of the I-frames encoded by CABCA. This method selects blocks having CBP values larger than one and chooses one among four AC highest-frequency coefficients whose LI falls between seven and nine. After selecting the watermarking positions, LSB replacement is performed with the chosen coefficients.

Table 8 highlights the performance of the considered LSB data hiding techniques in the compressed domain of videos. Overall, the works on LSB data hiding in the compressed domain focus mainly on effectively obtaining capacity while maintaining the imperceptibility of the hidden data. In general, subject to acceptable visual quality, the capacity that can be achieved in the compressed domain is lower than in the raw domain. On the other hand, good performance in terms of robustness and undetectability can be provided in the compressed domain.

4.3. Applications

In this section, selected applications of LSB data hiding in videos are presented. The related LSB-based data hiding algorithms focus on two main applications: Video authorization and secure transmission.

Video Authorization: In [261], a watermarking framework for surveillance videos is introduced. Privacy information is obtained from an identity sensor, compressed, and embedded into selected DCT coefficients belonging to the foreground regions of the video frames. This framework allows the management of users for video surveillance systems in restricted environments. The privacy of the authorized manager is protected securely and reliably while the access of unauthorized persons can be detected and rejected. In [262], a video copyright protection system is designed and implemented. The system applies LSB replacement to the DC coefficients of the I-frames of MPEG-4 cover videos. The LabVIEW developing environment is used to design the system with multiple digital watermarking for different subjects such as publishers, dealers, and buyers. This system protects video integrity and detects piracy.

Secure Transmission: In [263], LSB steganography for videos is applied to protect the confidentiality, integrity, and authentication of the concurrent version system (CVS) used for exchanging confidential documents and codes during software development. A parallel data structure is stored securely and secretly in MPEG-4 videos and uploaded to an organization file server. Users working remotely can access the server, read, modify, and update the secret documents embedded in the stego-videos. The server is synchronized so that the users always use the latest version of the collaborative documents. This system is helpful for working online and remotely. Apart from using LSB data hiding for establishing secure transmission, it can also be used for improving the error resilience against transmission errors. In [264], two LSB-based error-resilient video coding schemes are proposed for videos given in the H.263+ encoding format. The secret information characterizing each encoded macroblock (MB) comprises the data length of the MB, coding types for MBs, and the position of the MB in the group of blocks (GOB) which is used to improve the video synchronization. A corrupted MB is skipped at the decoder such that the decoding of the next MB is not affected by the transmission errors caused to previous blocks. For intra-MBs, the secret bits replace the LSB and second LSB of the quantized DC coefficients while these bits are covered in the first and second AC coefficients for inter-MBs. This scheme reduces the bit error rate considerably without significant increase in transmission bit rate.

5. LSB Data Hiding in 3D Media

This section provides a review of LSB data hiding methods for 3D media with respect to the classification shown in Fig. 2. 3D media represent data in three-dimensional space or visualize data so that viewers have space perception. 3D mesh models are examples of presenting a 3D digital object, which uses vertices, edges, and faces to form the shape of space and spatial features. 3D videos produced by computer-generated imagery (CGI) technology use geometric objects and 3D mesh models to present 3D animation and effects. Another way of showing 3D media is anaglyph 3D visualization, which combines 2D elements to give viewers a 3D perception of the observed object or scene. For example, a stereoscopic image can result from simultaneously presenting two 2D images of the same scene with two different views or two color components. Depth-image-based rendering (DIBR) images are created by combining a color 2D image and its related depth information. Anaglyph 3D media can be seen in multi-view color and multi-view

Table 8. Performance of LSB data hiding in the compressed domain of videos

Reference	Capacity	Imperceptibility	Robustness	Detectability	Security
[245]	1 bpnzc	–	–	–	–
[246]	–	PSNR > 18 dB	corrects transmission error using data hidden	–	–
[247]	1 bpnzc	PSNR > 28 dB	–	–	–
[248]	–	PSNR > 30 dB SSIM > 0.98	robust against a wide range of quantization parameter	–	–
[249]	–	PSNR > 35 dB	fragile under compression	–	encrypts secret data, randomizes hiding positions
[250]	–	PSNR > 35 dB	–	–	stego-video is encrypted before being transmitted
[243]	0.5 bit per IPM	–	–	reduces detection accuracy	scrambles secret data, randomizes hiding positions
[251]	–	PSNR > 40 dB	–	–	–
[252]	2 bpcmv	P frames: PSNR ∈ [20, 60] dB B frames: PSNR ∈ [15, 40] dB	–	–	–
[253]	1 bpcmv	PSNR > 26 dB	–	resists AoSO [257] steganalysis	–
[244]	1 bpcmv	PSNR > 34 dB	–	resists AoSO [257] and SPOM [258] steganalysis	–
[254]	0.5 bpmv	PSNR > 33 dB	–	resists motion vector based steganalysis in [259, 260]	–
[255]	1 bit per lc-VLC	PSNR ≈ 37 dB	–	–	–
[256]	–	PSNR > 36 dB	ER < 5 % under certain attacks[1]	–	–

[1] Gaussian noise addition, cropping, sharpening, blurring, and geometric modifications

(a) 3D mesh model ©[2019]IEEE. Reprint with permission, from [265].

(b) Anaglyph 3D image

(c) ERP video frame

Figure 9. Examples of 3D media: (a) 3D mesh model, (b) Anaglyph image, (c) Video frame in ERP format.

plus depth video systems. A third way of presenting 3D media is 360° media, also known as omnidirectional, surround, immersive, or spherical media. In this type of 3D media, flat high-resolution images or the frames of videos are rendered on a spherical surface around the viewer. Examples of a 3D mesh model, anaglyph 3D image, and a 360° video frame in equirectangular project (ERP) format are shown in Fig. 9.

5.1. 3D Mesh Media

The current LSB data hiding techniques in 3D mesh models have been performed primarily with respect to vertex coordinates. In [266], the x-, y-, and z-coordinate of 3D images in virtual reality modeling language (VRML) models are used separately to cover secret bits with the LSB$^+$ technique. Although originally proposed for images in [267] using the adjacent bin mapping method, the LSB$^+$ technique can also be applied to the coordinates of vertices for keeping the distribution of 0s and 1s in bit planes used for data hiding unchanged. All coordinates of the cover object are divided into non-overlapping bins of equal size. Each pair of two adjacent bins forms an embedding unit presenting bit 0 (left bin) and 1 (right bin). For covering a bit value of 0, the coordinate will be kept at its original position, if it belongs to the left bin, or mapped to the left bin if it is in the right bin. A similar process is followed for embedding a bit value of 1. The order of coordinates in the cover object is stored and exchanged between the sender and receiver for extraction. The hiding position

map may be scrambled with a secret key to enhance confidentiality. Given this order, the secret bits can be extracted easily from the positions of coordinates in the stego-object.

The work in [268] proposes a high capacity data hiding scheme for 3D geometric models by exploring triangle surface characteristics. In this scheme, a stego-key is generated from the secret message to be embedded. A decomposition ratio is calculated from the stego-key and used to construct triangle meshes by bifurcating the edges of an initial triangle. Specifically, the bifurcation generates more vertices in the edges of an initial triangle surface in a 3D image with a decomposition ratio computed from the secret message. As such, an initial triangle is segmented into many smaller triangles with additional vertices being added each time bifurcation is performed. The secret message is then embedded into the vertices of these triangles. For this purpose, the vertices of the triangles are labeled with one bit per vertex using the binary stego-key bits. Depending on whether the vertex label is 0 or 1, respectively, two secret bits are embedded in two LSBs of the vertex, or three secret bits are embedded in three LSBs of the vertex. Apart from providing high capacity, this data hiding scheme has been shown robust against cropping, rotation, scaling, translation, sharpening, noise addition, and filtering attacks.

In [269], LSB data hiding is applied to vertices of encrypted 3D mesh models for content protection. In this work, the coordinates of scrambled vertices are categorized into "embedded" and "referenced" sets. All adjacent vertices of the vertex belonging to the "embedded" set must be in the "referenced" set. The vertices in the "embedded" set are used to hide data, while those of the "referenced" set are not modified for recovering the original mesh at the receiver. The secret bits are covered in m LSBs of three encrypted coordinates of "embedded" vertices using the XOR operation. Error-correcting codes, including BCH, low-density parity-check (LDPC) [270], and Golay [271] codes, can be used to encode the message before being embedded.

Although 2D quality assessment metrics, e.g., SNR and PSNR, may be extended to 3D media, there is a need for metrics specifically tailored to assess the degradation of 3D mesh models under the data hiding process because of their complex structures. Current studies use several other measures to assess impairments to 3D mesh media caused by LSB modification. The work in [272] uses the term of dithered quantization to refer to the modification of vertex coordinates. Changing LSBs of the vertex coordinates is considered similar to adding noise. An expectation function of the angle between the triangle surface before and after the data hiding process is used to measure the degradation of LSB modification. A quantization level of each triangle is computed for a given degradation tolerance value based on this expectation function. The LSB data hiding for the 3D mesh model is performed into selected 32-bit vertices. A number of most significant bits, which is defined by the quantization level, is kept unchanged. The LSB is used to cover information of the quantization level, while the MSBs are replaced by message bits.

In [265], the term distortion, which refers to changes caused by the bit flipping operation on the cover vertex coordinates, is used to assess adaptive LSB data hiding. The work uses statistical features of the 3D mesh model, which includes mesh discriminative features [275], vertex normal features, curvature features [276], and sphere coordinate features. The Fisher linear discriminant analysis is used to determine their significance for detecting given embedding changes. Each feature is then associated with a weight contributing to a distortion function that measures the quality degradation caused by the data hiding process. Given the different impacts on the quality degradation, each 32-bit vertex coordinate is divided into unmodified, embedded, and invalid regions. The invalid region is usually fixed to 8 LSBs equal to zeros because modification in this region is noticeable. The width of the embedded region is varied, which depends on the length of the secret message and the number of vertices. LSB replacement is performed in all bit planes of the embedded region except the top bit plane which covers adaptively a small number of secret bits encoded by STCs [55] according to the distortion function.

Table 9 summarizes the performance of LSB data hiding techniques in 3D mesh media. These approaches generally have the potential of providing high capacity due to the enormous number of vertices. Several performance measures related to 3D media have been considered to maximize capacity while maintaining acceptable quality. Secure key generation and message encryption ensure strong security. On the other hand, robustness in terms of error rate is always fragile as an inherent weakness while little has been reported on detectability. Apart from vertex coordinates, there exist many other spatial aspects such as edges, surfaces, and mesh topology that show potential for data hiding as mentioned in the surveys [39, 40]. Furthermore, as suggested in [277] in the context of watermarking, the spatial points on a 3D-mesh object may be processed using spherical wavelet transform to obtain coefficients in the transform domain that could be used for LSB data hiding. Future research may consider this large variety of characteristics in the spatial and transform domain of 3D media represented in the form of 3D mesh models for LSB data hiding.

Table 9. Performance of LSB data hiding related to 3D mesh models

Reference	Capacity	Imperceptibility	Robustness	Detectability	Security
[265]	–	–	–	average testing error close to 0.5	–
[266]	0.1062 – 0.5066 bits/coordinate	3D SNR ≥ 60 dB	–	–	–
[268]	2 – 3 bpv	PSNR ≥ 55 dB	NC: (1) ≥ 0.87, (2) 1, (3) > 0.83, (4) > 0.87, (5) > 0.94, (6) > 0.91, (7) > 0.86	–	generation of stego-key depends on the secret message
[269]	[1] 0.3692 bpv [2] 0.3472 - 0.3508 bpv [3] 0.3413 - 0.3809 bpv	SNR = 31.97 % SNR ∈ [- 3.46, -2.84] SNR ∈ [25.03, 35.20]	ER = 4.22 % [a], < 2.11 % [b] ER ∈ [9.72 %, 11.39 %] [a] ER < 1.1 % [a]	–	data hiding positions are selected by a stego-key
[272]	37.61 – 68.26 bpv	average normal degradation ≤ 10°	–	–	–

Attacks: (1) Scaling, (2) Rotation, (3) Cropping, (4) Translation, (5) Sharpening, (6) Media filter, (7) Gaussian filter

[1] Test with the Stanford 3D scanning repository dataset [273], [2] test with the Princeton shape benchmark dataset [274] , [3] test with hand-made CAD meshes

[a] Without error correcting codes, [b] with error correcting codes

5.2. Anaglyph 3D Media

Because anaglyph 3D media are constructed from 2D elements, all LSB data hiding techniques reported in Section 3 and Section 4 for images and videos can be utilized in anaglyph 3D media.

Regarding anaglyph 3D images, the content correlation between the left-view and right-view images can be explored to design advanced LSB methods. In [278], a stereo image watermarking scheme with self-recovery capability is proposed, which exploits the inter-view relationship between the left-view and right-view images. The left-view and right-view images are divided into non-overlapping blocks of 4×4 pixels and two LSBs of each pixel in the obtained blocks are set to zero. These modified blocks are then transformed into four subbands by 1-level 2D-DWT, i.e., the LL, LH, HL, and HH subband. A block matching method based on the disparity between the blocks of the stereo image pair is used to classify all blocks in the left and right view into matched and unmatched blocks. With this classification, recovery reference bits are calculated from the differences between the coefficients of the LL subband, and the authentication bits are computed from the LH and HL subbands. A complex scheme including a secret key in combination with pseudo-random sequences is used for embedding reference bits, authentication bits, and the watermark of distinct LSBs in the matched and unmatched blocks. This stereo image watermarking scheme detects general tamper and resists collage attack. The work in [279] uses a chaotic function to generate authentication bits and a disparity map between the left and right views to support recovering tampered regions. The high-frequency energy, computed by summing all DWT coefficients of the HL, LH, and HH subbands, is used to classify the blocks into smooth and complex types and to compute the recovery reference bits. In addition, a just-noticeable difference (JND) model is used to distinguish sensitive and insensitive blocks of the left and right views. The JND guides the watermark embedding such that a trade-off between capacity and imperceptibility is achieved. The watermarking algorithm hides secret data of the left-view image into the right-view image and vice versa. Two LSBs of the pixels in the sensitive blocks and three LBSs of the pixels in the insensitive blocks are used for watermark embedding. The experimental results show that this asymmetric self-recovery method is capable to efficiently reconstruct tamper outperforming seven other stereo image watermarking methods. A reversible LSB data hiding method is proposed in [280], which also exploits the content correlation or similarity between the left-view and right-view images. Each image is divided into blocks of 8×8 pixels and transformed into low-, middle-, and high-frequency DCT coefficients which are called search, embedding, and non-used areas. Because the HVS is less sensitive to noise in the middle-frequencies compared to the low-frequencies, this proposed scheme maintains good image quality. Similar block pairs are found based on the search area. Secret data is then embedded in certain embedding areas of one of the similar block pairs. A stego-key is used to randomly choose the embedding image for each secret data embedding. In this work, each 3 bit secret data is converted into integers −1, 0, or +1, which are then embedded in the DCT-quantized coefficients of the appropriate embedding area with the absolute change of value being at most 1. This LSB data hiding method offers reversibility and high capacity.

LSB data hiding in anaglyph 3D media can also be performed with respect to cyan and red image or video frame components, or the color image or video frames. In [281], a two-layer LSB watermarking

technique is proposed using the spatial and transform domains for the left-view and right-view color video. In particular, the original anaglyph 3D video is divided into a sequence of frames which are then split into cyan and red images. A first mark or signature is embedded in each red image by replacing its LSBs by the most significant bits of the first mark. The same mark is hidden into the middle-frequency DCT coefficients of the cyan image. The two color components are then combined to form anaglyph frames that carry the first mark. A second mark is then embedded into these watermarked anaglyph frames using DWT embedding in the LL subband DWT coefficients to enhance the authentication of the anaglyph 3D video. This watermarking scheme is invisible and robust against geometric attacks, additional noise, filtering, frame-based attacks, and different video compression formats. In [282], a hybrid scheme using the DWT and the middle significant bit embedding (MIDSB) technique is proposed for improving the robustness of watermarks against collusion attacks. In this approach, the anaglyph 3D video is grouped into batches of 25 frames from which sprites (mosaic images) are generated, containing all data spread in the video sequence. The mark to be embedded in the sprites is spread to match the sprite size and then both, the spread mark and the sprite, are decomposed into subbands using 3-level DWT. The HL_3 and HH_3 coefficients of the mark are added to the HL_3 and HH_3 coefficients of the sprite subject to an invisibility factor. To maximize robustness against compression attacks, the spread mark is also embedded in the LL_3 and LH_3 coefficients of the sprite using MIDSB embedding. The marked sprites are then obtained from the modified subbands using the inverse DWT from which the marked 3D anaglyph video is reconstructed. Experimental results are provided, showing that the proposed approach is robust against several attacks while maintaining high visual quality.

A comparison of the performance of the above LSB data hiding methods in 3D anaglyph media is provided in Table 10. Taking advantages of the LSB data hiding in 2D images and videos, the discussed works in 3D anaglyph media have good performance in terms of imperceptibility. The watermarking techniques have good imperceptibility, strong robustness under certain attacks, and some of them provide effective detectability within reasonable security, which is helpful for tamper detection and prevention. The steganography methods have low detectability, i.e., pass Chi-square attack, and maintain acceptable imperceptibility. As such, LSB data hiding can be applied successfully in 3D anaglyph media if the relationship between the left-view and right-view images is carefully considered.

5.3. 360° Media

360° media are typically communicated, processed, and stored using a format obtained from projecting the sphere to the 2D plane while their 3D representations are used in rendering and displaying. Therefore, LSB data hiding schemes advised for conventional images and videos can be applied to the projected 2D formats of 360° media. It should be mentioned that sphere-to-plane projections induce a warping effect with distortions more pronounced at the poles in the 2D plane compared to the equator region in the 2D plane. On the other hand, distortions in the pole regions of the 2D plane are shrunk into small areas in the poles of the sphere causing negligible impairments. Apart from utilizing this characteristic of warping, mechanisms of the HVS are also exploited to improve the imperceptibility of LSB data hiding in 360° media. However, so far, LSB data hiding in projected formats of 360° images and videos have mainly been applied to the spatial domain.

In [283], LSB data hiding is performed using the spatial domain of ERP frames of a 360° video at different latitudes from North to South poles. As viewers put more attention to the areas around the equator region of a 360° video compared to the pole regions, LSB data hiding is performed in the regions around the poles without causing perceptually significant quality degradation. Because the ERP produces a large amount of data redundancy in the areas near the poles, increased capacity is available in the pole regions. The capacity can be controlled through the number of lines per frame, number of bit planes (LSB to the b-th LSB), or both number of lines per frame and bit planes used for data hiding. The video fidelity of the obtained 360° stego-videos is assessed in terms of the weighted-to-spherically-uniform PSNR (WS-PSNR) and the Craster parabolic projection PSNR (CPP-PSNR), which account for the warping effect of the ERP format. The numerical results show that video fidelity is kept high as long as the LSB data hiding is performed in the areas around the poles.

To allow using the mid-region around the equator for LSB data hiding, the work of [283] is extended in [284] by using morphological operations in the mid-region, which broadens the edge area for embedding secret data. This approach is motivated by the fact that the HVS is less sensitive to sharp intensity changes in the edge regions of an image or video frame. The numerical results illustrate the trade-offs between capacity and quality, which can be controlled by the number of lines in the pole regions, the size of the structuring element in the mid-region, and the number of bit planes used in the different regions.

In [285], the distribution of viewing direction frequency in both latitude and longitude are used to

Table 10. Performance of LSB data hiding related to anaglyph 3D media

Reference	Capacity	Imperceptibility	Robustness	Detectability	Security
[278]	–	PSNR ∈ [28, 57.81] dB under certain attacks[1]	self-recovery capability against collage and cropping attacks	probabilities of tamper detection ≥ 99 %	adaptive hiding based on left/right-view image matching
[279]	–	PSNR > 40 dB	self-recovery capability against pasting and cropping attacks	be detected easily for tamper prevention	classifies blocks with JND for adaptive hiding
[280]	0.12 - 0.38 bpp	PSNR > 30 dB	–	undetectable under Chi-square attack	–
[281]	–	PSNR > 62 dB	NC ≥ 0.97 under certain attacks[2]	–	–
[282]	–	PSNR ∈ [50, 58] dB	average NC ≥ 0.915, average BER < 0.007 under collusion and some certain attacks[2]	–	–

[1] Pasting, collage, and cropping attacks

[2] Geometric, noise, frame-based, enhancement, and compression attacks

define data hiding weight functions that control the amount of data to be hidden in different regions of 360° videos. This approach is motivated by the finding that humans view the front region near the equator much more often than other 360° video regions, i.e., the pole regions, and the west and east regions away from the front region. In particular, normalized Gaussian mixture models of the viewing behavior of humans are used for defining LSB data hiding weight functions for latitude, longitude, and both latitude and longitude. The total capacity obtained with this viewing direction based LSB data hiding scheme range from 1.74 to 172.04 Mbits/frame depending on the number of bit planes used. The wide range of total capacities allows for trading off capacity versus quality, i.e., hiding a sufficient amount of data in each 360° video while visual quality is kept at a satisfactory level.

A comparison of the performance of the above LSB data hiding methods in 360° media is provided in Table 11. LSB data hiding is performed addressing several scenarios in the first three studies where capacity is traded off with 360° video quality. It can be concluded that LSB data hiding methods used in 2D visual media can be extended to projected frames of 360° videos. In these methods, the projections' warping effect, user's viewing behaviors, and mechanisms of the HVS can be utilized.

Although LSB data hiding in 360° media seems at an early stage, it has been applied to some specific applications and may be expanded further to the following applications.

Geographic information system (GIS): In [286], LSB data hiding is applied to hide GIS metadata into the raster image of the GIS service-oriented architecture to ensure the synchronization of data retrieval during visualizing, manipulating, and interpreting 3D objects. In this work, up to four bit planes of pixel intensities in the raster map can be used to contain vector data, which resolves the problems of inefficient data transmission for GIS visualization.

360° *video surveillance system (360° VSS):* Data hiding techniques have already been applied to VSSs for authorization, access control, and privacy protection in [287, 288]. User information is embedded in each video frame to cover authorized users when the VSS is recording the scene. This type of systems protects the privacy of the authorized persons while monitoring the unauthorized persons in a restricted environment. Privacy information is only revealed in a secure way to the authorities or under special conditions. In view of the development of 360° VSSs, schemes offering security for such systems are needed. In [289], data hiding and watermarking methods are integrated into a conceptual framework for securing 360° VSS. However, due to the conceptual nature of this work, technical details on concealing private information into the background of video frames, or hiding and protecting private information in an entire video frame or different viewports are not provided. LSB data hiding may provide light-weight solutions to serve such tasks.

Near field communication (NFC) security: In [290], an NFC secured connection between smartphones is established by using LSB data hiding in 360° images. Secret data is encrypted by the receiver's international mobile equipment identity (IMEI) number as a key, embedded into the 360° image by LSB substitution, and sent to the receiver through the NFC channel. The authorized receiver can extract the secret data with its unique IMEI; otherwise, without proper stego-key, only the 360° stego-image is displayed.

Secure data storage and retrieval: VR, AR, and other types of immersive media services combine various services to improve users' experiences. Primary and additional services should be stored securely and retrieved accurately, requiring large storage space, effective data management, and a reliable access mechanism. Because of the large sizes of 360° images and videos, applying LSB data hiding in these media may satisfy these requirements. In [291], hiding human voice, portrait data, and metadata into 360° images

is proposed using LSB data hiding. The secret data is covered in the LSB of each non-zero DCT coefficient of the 360° cover image while different regions can contain different information. The additional data will be played out with respect to the current viewport during watching the 360° image on a head-mounted display (HMD). Thus, the additional services communicated within the 360° stego-image can be synchronized securely with the immersive media services while they do incur additional costs in terms of storage space and bandwidth.

6. Conclusions and Future Research Directions

In this paper, we have provided a comprehensive survey on LSB data hiding in digital media. In contrast to previous surveys on data hiding in digital media, which have focused on one particular digital medium but for a wide range of data hiding methods, this survey has been dedicated to LSB data hiding for digital audio, image, video, and 3D media. Given the tremendous developments in digital media communications ranging from conventional digital audio to immersive media, LSB data hiding plays an important role in providing high capacity and maintaining imperceptibility by considering mechanisms of the HAS and HVS. In view of future applications in even more advanced immersive media toward the metaverse, LSB data hiding methods also offer the benefit of keeping computational load for embedding secret data and the associated latency low.

This survey on LSB data hiding in digital media has provided fundamentals of data hiding including the general data hiding model and the related terminologies. The attributes of data hiding techniques used in this survey for performance comparison of the wide range LSB data hiding methods are described, i.e., capacity, imperceptibility, robustness, detectability, and security. An overview of performance metrics associated with these attributes is also given. In addition, a detailed overview of contemporary surveys on data hiding in digital media has been presented showing the lack of a dedicated survey on LSB data hiding in digital media. On this basis, a classification of LSB data hiding techniques has been provided which serves as a foundation of addressing the related techniques for digital audio, image, video, and 3D media. The survey of LSB data hiding is then conducted for each of the four digital media with respect to its specific data hiding domains along with a summary of the performance of the considered techniques. The main takeaways of this survey may be summarized as follows:

- This survey has revealed that LSB data hiding has indeed gained tremendous use in digital audio, image, video, and 3D media.
- Regarding LSB data hiding in audio, large capacity and good quality can be obtained in the temporal domain while robustness against noise and data processing is low. Performance improvements in terms of detectability and security can be achieved by combining LSB data hiding with cryptography. In contrast, in the transform domain of audio, capacity is generally lower compared to the temporal domain while imperceptibility, robustness, and detectability related performance improves. However, there seems to be a lack of studies on security related to confidentiality and integrity for the transform domain. As for as the coded domain of audio is concerned, imperceptibility, detectability and security are coped with well while capacity and robustness are relatively low.
- As far as LSB data hiding in images is concerned, similar as for the temporal domain in audio, high capacity can be offered while maintaining good visual quality. However, robustness against noise, data processing, and attacks is generally low with only a few reversible LSB data hiding algorithms addressing this problem. On the other hand, detectability can be minimized in the spatial domain which comes at the expense of reduced capacity. Alternatively, in the transform domain of images, given acceptable visual quality, capacity is considerably lower than in the spatial domain but a high level of robustness is provided making this domain used in many strong watermarking techniques. However, there exist only a few studies on detectability and security of LSB data hiding in the transform domain of images.
- A promising avenue for LSB data hiding techniques has occurred with the advent of quantum technology allowing to hide secret data in the quantum domain. This option has been focusing so far on spatial LSB replacement in the context of qubits where it has proven to provide high capacity, good visual image quality, good security using scrambling of secret bits while robustness and detectability performance is rather poor.
- LSB data hiding in the raw domain of videos has been largely focused on watermarking applications with the aim on accessing easily and effectively the watermark rather than concealing its existence. In general, in the raw domain of videos, large capacity is provided while keeping good visual quality and to some extent resisting noise and filtering attacks. Regarding the compressed domain, the main focus is given to provide high capacity while maintaining imperceptibility of the hidden data. In comparison to the raw

Table 11. Performance of LSB data hiding related to 360° media

Reference	Capacity	Imperceptibility	Robustness	Detectability	Security
[283]	0.1758 bpp/frame	30 dB < WS-PSNR < 65 dB 30 dB < CPP-PSNR < 65 dB	–	–	–
[284]	[a] 0.2 – 6.1 bpp/frame [b, c] 0.2 – 6.1 bpp/frame [b, d] 1.7 – 3.8 bpp/frame	[a] WS-PSNR > 23 dB [b, c] WS-PSNR > 23 dB [b, d] WS-PSNR > 23 dB	–	–	–
[285]	[1] 0.8307 – 4.9843 bpp/frame [2] 0.8393 – 5.0359 bpp/frame [3] 0.9723 – 5.8338 bpp/frame	[1] NCP-PSNR > WS-PSNR > PSNR > 20 dB [2] NCP-PSNR > WS-PSNR = PSNR > 20 dB [3, *] NCP-PSNR ∈ [50, 100] dB [1, 2, 3] NCP-SSIM > SSIM	–	–	–
[290]	1 bpp	PSNR > 85 dB	–	–	secret data is encrypted
[291]	1 bpnzc	PSNR > 50 dB	–	–	–
Data hiding strategies are performed: [a] at the pole regions, [b] at the pole regions and at the mid-region					
Data hiding strategies are performed in the mid-region: [c] with only LSB used, [d] with bit planes used from 1 to 6					
Data hiding weight functions versus: [1] latitude, [2] longitude, and [3] latitude and longitude					
* The number of bit planes used is less or equal to 3					

domain, the capacity in the compressed domain is generally lower but good performance is provided in terms of robustness and detectability.

- In contrast to audio, image, and video, LSB data hiding in 3D media is not as developed but has large scope for future work. In particular, LSB data hiding in 3D mesh models and 360° videos has so far been focusing on the spatial domain and studying trade-offs between capacity and imperceptibility while other attributes have been given little attention.

- This survey shows that LSB data hiding has been widely used in many different applications throughout all considered digital media and can therefore be expected to continue playing an important role within the field of information security for future digital media applications.

In view of the insights gained from this survey on LSB data hiding in digital media, promising directions for future work include the following:

- Although there have been initial works on improving the robustness of LSB data hiding with respect to source encoding of the temporal, raw, and spatial domain formats of digital media, more advanced methods are still needed. This applies in particular to upcoming and future mobile immersive media applications which require high capacity, robustness to compression algorithms, and low processing latency.

- Another promising field of research may be directed to further account for mechanisms of the HAS and HVS in the development of LSB data hiding techniques for digital media. In relation to visual stimuli, for example, the HVS operates on structural information rather than pixel-by-pixel comparisons, is guided by visual attention directing gaze to objects of interest in the visual scene, performs multiple-scale processing to adapt to visual information at different scales due to objects of different sizes or varying distances, and other mechanisms. These mechanisms may be used to provide high capacity while maintaining imperceptibility of the hidden data.

- LSB data hiding may be extended to audiovisual media to simultaneously utilize the options provided by the different domains of audio, image, video, and 3D media for LSB data hiding.

- Given the trend to more advanced 3D media applications, there is a strong need for new performance metrics that are better tailored to these types of digital media. In this context, ground truths about the impact of LSB data hiding on the different data hiding attributes may be produced through subjective experiments along with establishing public databases.

Acknowledgement. This work has been supported in part by The Knowledge Foundation, Sweden, through the ViaTecH project (Contract 20170056). Dang Ninh Tran has been supported by a VIED scholarship awarded by the Vietnamese Government.

References

[1] Cox IJ, Miller ML, Bloom JA. Digital watermarking and steganography. 2nd ed. Burlington, MA, USA: Morgan Kaufmann; 2008.

[2] Petitcolas FAP, Anderson RJ, Kuhn MG. Information hiding - A survey. Proceedings of the IEEE. 1999 Jul;87(7):1062-78.
[3] Wayner P. Disappearing cryptography: Information hiding: Steganography and watermarking. 3rd ed. Burlington, MA, USA: Morgan Kaufmann Inc.; 2008.
[4] Ni Z, Shi YQ, Ansari N, Su W. Reversible data hiding. IEEE Trans on Circuits and Systems for Video Technology. 2006 Mar;16(3):354-62.
[5] Zeng W. Digital watermarking and data hiding: Technologies and applications. In: Int. Conference on Information Systems, Analysis and Synthesis. Orlando, FL, USA; 1998. p. 223–229.
[6] Pfitzmann B. Information hiding terminology. In: Int. Workshop on Information Hiding. Cambridge, U.K.; 1996. p. 347-50.
[7] Zhang J, Marshall A, Woods R, Duong TQ. Efficient key generation by exploiting randomness from channel responses of individual OFDM subcarriers. IEEE Trans on Communications. 2016 Jun;64(6):2578-88.
[8] Zhang J, Duong TQ, Marshall A, Woods R. Key generation from wireless channels: A review. IEEE Access. 2016 Jan;4:614-26.
[9] Johnson NF, Duric Z, Jajodia S. Information hiding: Steganography and watermarking - Attacks and countermeasures. 1st ed. Boston, MA, USA: Springer; 2001.
[10] Kalker T. Considerations on watermarking security. In: IEEE Workshop on Multimedia Signal Processing. Cannes, France; 2001. p. 201-6.
[11] Cachin C. An information-theoretic model for steganography. Information and Computation. 2004 Jul;192(1):41-56.
[12] Hopper N, von Ahn L, Langford J. Provably secure steganography. IEEE Trans on Computers. 2009 May;58(5):662-76.
[13] Nyeem H, Boles W, Boyd C. A review of medical image watermarking requirements for teleradiology. J of Digital Imaging. 2013 Apr;26(2):326-43.
[14] Grībermans D, Jeršovs A, Rusakovs P. Development of requirements specification for steganographic systems. Applied Computer Systems. 2016 Dec;20(1):40-8.
[15] Iwamuar K, Kawamura M, Kuribayashi M, Iwata M, Kang H, Gohshi S, et al. Information hiding and its criteria for evaluation. IEICE Trans on Information and Systems. 2017 Jan;E100.D:2-12.
[16] Liśkiewicz M, Reischuk R, Wölfel U. Security levels in steganography – Insecurity does not imply detectability. Theoretical Computer Science. 2017 Sep;692:25-45.
[17] Ke Y, Liu J, Zhang MQ, Su TT, Yang XY. Steganography security: Principle and practice. IEEE Access. 2018 Dec;6:73009-22.
[18] Roux JL, Wisdom S, Erdogan H, Hershey JR. SDR – Half-baked or well done? In: IEEE Int. Conference on Acoustics, Speech and Signal Processing. Brighton, UK; 2019. p. 626-30.
[19] Winkler S. Digital Video Quality - Vision Models and Metrics. Bridgewater, NJ, USA: John Wiley & Sons; 2005.
[20] Wang Z, Bovik AC, Sheikh HR, Simoncelli EP. Image quality assessment: From error visibility to structural similarity. IEEE Trans Image Processing. 2004 Apr;13(4):600-12.
[21] Recommendation ITU-T P 800. Methods for subjective determination of transmission quality. Geneva, Switzerland: International Telecommunication Union - Telecommunication Standardization Sector; 1996.
[22] Recommendation ITU-T P 862. Perceptual evaluation of speech quality (PESQ): An objective method for end-to-end speech quality assessment of narrow-band telephone networks and speech codecs. Geneva, Switzerland: International Telecommunication Union - Telecommunication Standardization Sector; 2001.
[23] Recommendation ITU-R BS 1387-1. Method for objective measurements of perceived audio quality. Geneva, Switzerland: International Telecommunication Union - Telecommunication Standardization Sector; 2001.
[24] Hedelin P, Norden F, Skoglund J. SD optimization of spectral coders. In: IEEE Workshop on Speech Coding Proceedings. Model, Coders, and Error Criteria. Porvoo, Finland; 1999. p. 28-30.
[25] Sencar HT, Ramkumar M, Akansu AN. Data hiding fundamentals and applications. 1st ed. San Diego, CA, USA: Elsevier Academic Press; 2004.
[26] Djebbar F, Ayad B, Meraim KA, Hamam H. Comparative study of digital audio steganography techniques. EURASIP J on Audio, Speech, and Music Processing. 2012 Oct;2012(1):1-16.
[27] Mazurczyk W. VoIP steganography and its detection — A survey. ACM Computing Surveys. 2013 Dec;46(2):20.
[28] Wu Z. Information hiding in speech signals for secure communication. 1st ed. Oxford , UK: Syngress; 2015.
[29] AlSabhany AA, Ali AH, Ridzuan F, Azni AH, Mokhtar MR. Digital audio steganography: Systematic review, classification, and analysis of the current state of the art. Computer Science Review. 2020 Nov;38:100316.
[30] Cheddad A, Condell J, Curran K, Kevitt PM. Digital image steganography: Survey and analysis of current methods. Signal Processing. 2010 Mar;90(2):727-52.
[31] Subhedar MS, Mankar VH. Current status and key issues in image steganography: A survey. Computer Science Review. 2014 Nov;13-14:95-113.
[32] Sreenivas K, Prasad VK. Fragile watermarking schemes for image authentication: A survey. Int J of Machine Learning and Cybernetics. 2018 Jul;9(7):1193-218.
[33] Kadhim IJ, Premaratne P, Vial PJ, Halloran B. Comprehensive survey of image steganography: Techniques, evaluations, and trends in future research. Neurocomputing. 2019 Mar;335:299-326.
[34] Subramanian N, Elharrouss O, Al-Maadeed S, Bouridane A. Image steganography: A review of the recent advances. IEEE Access. 2021 Jan;9:23409-23.
[35] Tew Y, Wong K. An overview of information hiding in H.264/AVC compressed video. IEEE Trans on Circuits and Systems for Video Technology. 2014 Feb;24(2):305-19.
[36] Sadek MM, Khalifa AS, Mostafa MGM. Video steganography: A comprehensive review. Multimedia Tools and Applications. 2015 Sep;74(17):7063-94.

[37] Mstafa RJ, Elleithy KM. Compressed and raw video steganography techniques: A comprehensive survey and analysis. Multimedia Tools and Applications. 2017 Oct;76(20):21749-86.
[38] Liu Y, Liu S, Wang Y, Zhao H, Liu S. Video steganography: A review. Neurocomputing. 2019 Mar;335:238-50.
[39] Girdhar A, Kumar V. Comprehensive survey of 3D image steganography techniques. IET Image Processing. 2018 Jan;12(1):1-10.
[40] Borah S, Borah B. Watermarking techniques for three dimensional (3D) mesh authentication in spatial domain. 3D Research. 2018 Aug;9(3):43.
[41] Collins JC, Agaian SS. Taxonomy for spatial domain LSB steganography techniques. In: SPIE Sensing Technology and Applications. vol. 9120. Baltimore, MD, US; 2014. p. 912006-1 912006-15.
[42] Jois A, Tejaswini L. Survey on LSB data hiding techniques. In: IEEE Int. Conf. on Wireless Communication, Signal Processing, and Networking. Chennai, India; 2016. p. 656-60.
[43] Smitha GL, Baburaj E. A survey on image steganography based on block-based edge adaptive based on least significant bit matched revisited (LSBMR) algorithm. In: Int. Conf. on Emerging Technology Trends. Kumaracoil, India; 2016. p. 1-6.
[44] Malathi P, Gireeshkumar T. Relating the embedding efficiency of LSB steganography techniques in spatial and transform domains. Procedia Computer Science. 2016;93:878-85.
[45] Bharti J, Solanki S, Beliya A. Comparison of LSB methods and pattern. In: Int. Conf. on Recent Innovations in Signal Processing and Embedded Systems. Bhopal, India; 2017. p. 250-6.
[46] Bansal K, Agrawal A, Bansal N. A survey on steganography using least significant bit (LSB) embedding approach. In: Int. Conf. on Trends in Electronics and Informatics. Tirunelveli, India; 2020. p. 64-9.
[47] Shtayt BA, Zakaria NH, Harun NH. A comprehensive review on medical image steganography based on LSB technique and potential challenges. Baghdad Science J. 2021 Jun:64-9.
[48] Tran DN. On LSB Data Hiding in New Digital Media. Karlskrona, Sweden: Blekinge Institute of Technology; 2020.
[49] Turner LF. Digital data security system [Patent]; WO/1989/008915. 1989 Sep. Available from: https://patentscope.wipo.int/search/en/detail.jsf?docId=WO1989008915.
[50] Cvejic N, Seppanen T. Increasing the capacity of LSB-based audio steganography. In: IEEE Workshop on Multimedia Signal Processing. St. Thomas, VI, USA; 2002. p. 336-8.
[51] Cvejic N, Seppanen T. Increasing robustness of LSB audio steganography by reduced distortion LSB coding. J of Universal Computer Science. 2005 Jan;11(1):56-65.
[52] Abdulrazzaq ST, Siddeq MM, Rodrigues MA. A novel steganography approach for audio files. SN Computer Science. 2020 Mar;1(2):97.
[53] Zamani M, Taherdoost H, Manaf AA, Ahmad RB, Zeki AM. Robust audio steganography via genetic algorithm. In: Int. Conf. on Information and Communication Technology. Karachi, Pakistan; 2009. p. 149-53.
[54] Zamani M, Manaf ABA. Genetic algorithm for fragile audio watermarking. Telecommunication Systems. 2015 Jul;59(3):291-304.
[55] Filler T, Judas J, Fridrich J. Minimizing additive distortion in steganography using syndrome-trellis codes. IEEE Trans on Information Forensics and Security. 2011 Sep;6(3):920-35.
[56] Ying K, Wang R, Lin Y, Yan D. Adaptive audio steganography based on improved syndrome-trellis codes. IEEE Access. 2021 Jan;9:11705-15.
[57] Kar DC, Mulkey CJ. A multi-threshold based audio steganography scheme. J of Information Security and Applications. 2015 Aug;23:54-67.
[58] Ali AH, George LE, Zaidan AA, Mokhtar MR. High capacity, transparent and secure audio steganography model based on fractal coding and chaotic map in temporal domain. Multimedia Tools and Applications. 2018 Dec;77(23):31487-516.
[59] Faragallah OS. Secure audio cryptosystem using hashed image LSB watermarking and encryption. Wireless Personal Communications. 2018 Jan;98(2):2009-23.
[60] Rivest R. RFC1321: The MD5 message-digest algorithm. Cambridge, MA, USA: MIT Laboratory for Computer Science and RSA Data Security, Inc; 1992.
[61] Advanced Encryption Standard (AES). Springfield, VA, USA: National Institute of Standards and Technology; 2001. FIPS PUB 197.
[62] Rivest RL, Robshaw MJB, Sidney R, Yin YL. The RC6 block cipher. In: First Advanced Encryption Standard (AES) Candidate Conference Report. Ventura, CA, USA; 1998. p. 1-21.
[63] Chen K, Yan F, Iliyasu AM, Zhao J. Exploring the implementation of steganography protocols on quantum audio signals. Int J of Theoretical Physics. 2018 Feb;57(2):476-94.
[64] Nejad MY, Mosleh M, Heikalabad SR. An LSB-based quantum audio watermarking using MSB as arbiter. Int J of Theoretical Physics. 2019 Aug;58:3828-51.
[65] Cvejic N, Seppanen T. A wavelet domain LSB insertion algorithm for high capacity audio steganography. In: Digital Signal Processing Workshop and Signal Processing Education Workshop. Pine Mountain, GA, USA; 2002. p. 53-5.
[66] Ballesteros L DM, Moreno A JM. Highly transparent steganography model of speech signals using efficient wavelet masking. Expert Systems with Applications. 2012 Aug;39(10):9141-9.
[67] Ballesteros L DM, Moreno A JM. Real-time, speech-in-speech hiding scheme based on least significant bit substitution and adaptive key. Computers and Electrical Engineering. 2013 May;39(4):1192-203.
[68] Delforouzi A, Pooyan M. Adaptive digital audio steganography based on integer wavelet transform. Circuits, Systems and Signal Processing. 2008 Apr;27(2):247-59.
[69] Pooyan M, Delforouzi A. LSB-based audio steganography method based on lifting wavelet transform. In: Int. Symp. on Signal Processing and Information Technology. Giza, Egypt; 2007. p. 600-3.

[70] Huang J, Wang Y, Shi YQ. A blind audio watermarking algorithm with self-synchronization. In: Int. Symp. on Circuits and Systems. vol. 3. Phoenix-Scottsdale, AZ, USA; 2002. p. III-627630.
[71] Bose RC, Ray-Chaudhuri DK. On a class of error correcting binary group codes. Information and Control. 1960 Mar;3(1):68-79.
[72] Bellaaj M, Ouni K. Audio watermarking technique in frequency domain: Comparative study MDCT vs DCT. Multimedia Tools and Applications. 2020 Oct;79(37):27161-84.
[73] Cheng MH, Hsu YH. Fast IMDCT and MDCT algorithms - A matrix approach. IEEE Trans on Signal Processing. 2003 Jan;51(1):221-9.
[74] Djebbar F, Ayad B, A -Meraim K, Hamam H. Unified phase and magnitude speech spectra data hiding algorithm. Security and Communication Networks. 2013 Jan;6(8):961-71.
[75] Liu Q, Sung AH, Qiao M. Temporal derivative-based spectrum and mel-cepstrum audio steganalysis. IEEE Trans on Information Forensics and Security. 2009 Sep;4(3):359-68.
[76] Salah E, Amine K, Redouane K, Fares K. A Fourier transform based audio watermarking algorithm. Applied Acoustics. 2021 Jan;172:107652.
[77] Wang XY, Zhao H. A novel synchronization invariant audio watermarking scheme based on DWT and DCT. IEEE Trans on Signal Processing. 2006 Dec;54(12):4835-40.
[78] Karajeh H, Maqableh M. An imperceptible, robust, and high payload capacity audio watermarking scheme based on the DCT transformation and Schur decomposition. Analog Integrated Circuits and Signal Processing. 2019 Jun;99(3):571-83.
[79] Karajeh H, Khatib T, Rajab L, Maqableh M. A robust digital audio watermarking scheme based on DWT and Schur decomposition. Multimedia Tools and Applications. 2019 Jul;78(13):18395-418.
[80] Ahani S, Ghaemmaghami S, Wang ZJ. A sparse representation-based wavelet domain speech steganography method. IEEE/ACM Trans on Audio, Speech, and Language Processing. 2015 Jan;23(1):80-91.
[81] Steinebach M, Petitcolas FAP, Raynal F, Dittmann J, Fontaine C, Seibel S, et al. StirMark benchmark: Audio watermarking attacks. In: Int. Conf. on Information Technology: Coding and Computing. Las Vegas, NV, USA; 2001. p. 49 54.
[82] Liu Q, Sung AH, Qiao M. Derivative-based audio steganalysis. ACM Trans Multimedia Computing, Communications, and Applications. 2011 Sep;7(3):18.
[83] Liu Y, Chiang K, Corbett C, Archibald R, Mukherjee B, Ghosal D. A novel audio steganalysis based on high-order statistics of a distortion measure with Hausdorff distance. In: Int. Conf. on Information Security. Taipei, Taiwan; 2008. p. 487-501.
[84] Recommendation ITU-T G 711. Pulse code modulation (PCM) of voice frequencies. Geneva, Switzerland: International Telecommunication Union - Telecommunication Standardization Sector; 1972.
[85] Aoki N. A packet loss concealment technique for VoIP using steganography. In: Int. Symp. on Intelligent Signal Processing and Communication Systems. Awaji Island, Japan; 2003. p. 470-3.
[86] Aoki N. VoIP packet loss concealment based on two-side pitch waveform replication technique using steganography. In: IEEE Region 10 Conference. Chiang Mai, Thailand; 2004. p. 52-5.
[87] Huang Y, Xiao B, Xiao H. Implementation of covert communication based on steganography. In: Int. Conf. on Intelligent Information Hiding and Multimedia Signal Processing. Harbin, China; 2008. p. 1512-5.
[88] Chen Z, Zhao C, Geng G, Yin F. An audio watermark-based speech bandwidth extension method. EURASIP J on Audio, Speech, and Mum-sesic Processing. 2013 Dec;2013(1):1-8.
[89] Recommendation ITU-T G 792. Characteristics common to all transmultiplexing equipments. Geneva, Switzerland: International Telecommunication Union - Telecommunication Standardization Sector; 1980.
[90] Tian H, Zhou K, Jiang H, Liu J, Huang Y, Feng D. An m-sequence based steganography model for voice over IP. In: IEEE Int. Conf. on Communication. Dresden, Germany; 2009. p. 1-5.
[91] Tian H, Zhou K, Jiang H, Huang Y, Liu J, Feng D. An adaptive steganography scheme for voice over IP. In: IEEE Int. Symp. on Circuits and Systems. Taipei, Taiwan; 2009. p. 2922-5.
[92] Tian H, Jiang H, Zhou K, Feng D. Adaptive partial-matching steganography for voice over IP using triple m-sequences. Computer Communications. 2011 Dec;34(18):2236-47.
[93] Yan S, Tang G, Sun Y, Gao Z, Shen L. A triple-layer steganography scheme for low bit-rate speech streams. Multimedia Tools and Applications. 2015 Dec;74(24):11763-82.
[94] Kheddar H, Bouzid M, Megías D. Pitch and Fourier magnitude based steganography for hiding 2.4 kbps MELP bitstream. IET Signal Processing. 2019 Jan;13(3):396-407.
[95] Johnson MK, Lyu S, Farid H. Steganalysis of recorded speech. In: SPIE Electronic Imaging. San Jose, CA, USA; 2005. p. 664-72.
[96] Fan M. A source coding scheme for authenticating audio signal with capability of self-recovery and anti-synchronization counterfeiting attack. Multimedia Tools and Applications. 2020 Jan;79(1):1037-55.
[97] Qian Q, Cui Y, Wang H, Deng M. REPAIR: Fragile watermarking for encrypted speech authentication with recovery ability. Telecommunication Systems. 2020 Nov;75(3):273-89.
[98] Wei Z, Zhao B, Liu B, Su J, Xu L, Xu E. A novel steganography approach for voice over IP. J of Ambient Intelligence and Humanized Computing. 2014 Aug;5(4):601-10.
[99] Linphone. Belledonne Communications; 2020. Available from: "https://www.linphone.org/technical-corner/linphone?qt-technical_corner=2#qt-technical_corner".
[100] Tang S, Jiang Y, Zhang L, Zhou Z. Audio steganography with AES for real-time covert voice over internet protocol communications. Science China Information Sciences. 2014 Feb;57(3):1-14.

[101] Sheikh JA, Akhter S, Parah SA, Bhat GM. Blind digital speech watermarking using filter bank multicarrier modulation for 5G and IoT driven networks. Int J of Speech Technology. 2018 Aug;21(3):715-22.
[102] Anguraj S, Shantharajah SP, Jeba EJ. A steganographic method based on optimized audio embedding technique for secure data communication in the internet of things. Computational Intelligence. 2020;36(2):557-73.
[103] Al-Juaid N, Gutub A. Combining RSA and audio steganography on personal computers for enhancing security. SN Applied Sciences. 2019 Jul;1(8):830.
[104] Rajamani K, Srideviponmalar P, Bebe PC, Samyuktha CT. Secured implementation of steganography in multicloud. Materials Today: Proceedings. 2020 Dec.
[105] Kurak C, Hugh JM. A cautionary note on image downgrading. In: Annual Computer Security Application Conference. San Antonio, TX, USA; 1992. p. 153-9.
[106] Lee YK, Chen LH. High capacity image steganographic model. IEE Proceedings - Vision, Image and Signal Processing. 2000 Jun;147(3):288-94.
[107] Wang RZ, Lin CF, Lin JC. Hiding data in images by optimal moderately-significant-bit replacement. Electronics Letters. 2000 Dec;36(25):2069-70.
[108] Wang RZ, Lin CF, Lin JC. Image hiding by optimal LSB substitution and genetic algorithm. Pattern Recognition. 2001 Mar;34(3):671-83.
[109] Banharnsakun A. Artificial bee colony approach for enhancing LSB based image steganography. Multimedia Tools and Applications. 2018 Oct;77(20):27491-504.
[110] Chan CK, Cheng LM. Hiding data in images by simple LSB substitution. Pattern Recognition. 2004 Mar;37(3):469-74.
[111] Lin IC, Lin YB, Wang CM. Hiding data in spatial domain images with distortion tolerance. Computer Standards and Interfaces. 2009 Feb;31(2):458-64.
[112] Yang CH. Inverted pattern approach to improve image quality of information hiding by LSB substitution. Pattern Recognition. 2008 Aug;41(8):2674-83.
[113] Behnia S, Teshnehlab M, Ayubi P. Multiple-watermarking scheme based on improved chaotic maps. Communications in Nonlinear Science and Numerical Simulation. 2010 Sep;15(9):2469-78.
[114] Kanso A, Own HS. Steganographic algorithm based on a chaotic map. Communications in Nonlinear Science and Numerical Simulation. 2012 Aug;17(8):3287-302.
[115] Das SK, Dhara BC. An LSB based novel data hiding method using extended LBP. Multimedia Tools and Applications. 2018 Jun;77(12):15321-51.
[116] Wu HC, Wu NI, Tsai CS, Hwang MS. Image steganographic scheme based on pixel-value differencing and LSB replacement methods. IEE Proceedings - Vision, Image and Signal Processing. 2005 Oct;152(5):611-5.
[117] Yang CH, Weng CY, Wang SJ, Sun HM. Varied PVD + LSB evading detection programs to spatial domain in data embedding systems. J of Systems and Software. 2010 Oct;83(10):1635-43.
[118] Sharp T. An implementation of key-based digital signal steganography. In: Int. Workshop on Information Hiding. Pittsburgh, PA, USA; 2001. p. 13-26.
[119] Ker AD. Resampling and the detection of LSB matching in color bitmaps. In: SPIE Electronic Imaging. San Jose, CA, USA; 2005. p. 1-15.
[120] Mielikainen J. LSB matching revisited. IEEE Signal Processing Letters. 2006 May;13(5):285-7.
[121] Li X, Yang B, Cheng D, Zeng T. A generalization of LSB matching. IEEE Signal Processing Letters. 2009 Feb;16(2):69-72.
[122] Wong PW. A watermark for image integrity and ownership verification. In: Image Processing, Image Quality, Image Capture, Systems Conference. Portland, OR, USA; 1998. p. 374-9.
[123] Wong PW. A public key watermark for image verification and authentication. In: Int. Conf. on Image Processing. Chicago, IL, USA; 1998. p. 455-9.
[124] Fridrich J. Security of fragile authentication watermarks with localization. In: SPIE Electronic Imaging. San Jose, CA, USA; 2002. p. 691-700.
[125] Shanthakumari R, Malliga S. Dual layer security of data using LSB inversion image steganography with elliptic curve cryptography encryption algorithm. Multimedia Tools and Applications. 2019 Apr:1-17.
[126] Honsinger CW, Jones PW, Rabbani M, Stoffel JC. Lossless recovery of an original image containing embedded data. Eastman Kodak Company; 2001. Patent: US 6,278,791 B1.
[127] Celik MU, Sharma G, Tekalp AM, Saber E. Lossless generalized-LSB data embedding. IEEE Trans on Image Processing. 2005 Feb;14(2):253-66.
[128] Celik MU, Sharma G, Tekalp AM. Lossless watermarking for image authentication: A new framework and an implementation. IEEE Trans on Image Processing. 2006 Apr;15(4):1042-9.
[129] Chang CC, Kieu TD, Chou YC. Reversible data hiding scheme using two steganographic images. In: IEEE Region 10 Conference. Taipei, Taiwan; 2007. p. 1-4.
[130] Lu TC, Tseng CY, Wu JH. Dual imaging-based reversible hiding technique using LSB matching. Signal Processing. 2015 Mar;108:77-89.
[131] Sahu AK, Swain G. Reversible image steganography using dual-layer LSB matching. Sensing and Imaging. 2020 Dec;21(1):1-21.
[132] Yang CH, Weng CY, Wang SJ, Sun HM. Adaptive data hiding in edge areas of images with spatial LSB domain systems. IEEE Trans on Information Forensics and Security. 2008 Sep;3(3):488-97.
[133] Liao X, Wen QY, Zhang J. A steganographic method for digital images with four-pixel differencing and modified LSB substitution. J of Visual Communication and Image Representation. 2011 Jan;22(1):1-8.
[134] Jung KH, Yoo KY. Data hiding using edge detector for scalable images. Multimedia Tools and Applications. 2014 Aug;71(3):1455-68.
[135] Dadgostar H, Afsari F. Image steganography based on interval-valued intuitionistic fuzzy edge detection and modified LSB. J of Information Security and Applications. 2016 Oct;30:94-104.
[136] Chakraborty S, Jalal AS, Bhatnagar C. LSB based non-blind predictive edge adaptive image steganography. Multimedia Tools and Applications. 2017 Mar;76(6):7973-87.

[137] Ghosal SK, Mandal JK, Sarkar R. High payload image steganography based on Laplacian of Gaussian (LoG) edge detector. Multimedia Tools and Applications. 2018 Dec;77(23):30403-18.
[138] Ioannidou A, Halkidis ST, Stephanides G. A novel technique for image steganography based on a high payload method and edge detection. Expert Systems with Applications. 2012 Oct;39(14):11517-24.
[139] Chen WJ, Chang CC, Le THN. High payload steganography mechanism using hybrid edge detector. Expert Systems with Applications. 2010 Apr;37(4):3292-301.
[140] Bai J, Chang CC, Nguyen TS, Zhu C, Liu Y. A high payload steganographic algorithm based on edge detection. Displays. 2017 Jan;46:42-51.
[141] Luo W, Huang F, Huang J. Edge adaptive image steganography based on LSB matching revisited. IEEE Trans on Information Forensics and Security. 2010 Jun;5(2):201-14.
[142] Al-Dmour H, Al-Ani A. A steganography embedding method based on edge identification and XOR coding. Expert Systems with Applications. 2016 Mar;46:293-306.
[143] Khan S. Ant colony optimization (ACO) based data hiding in image complex region. Int J of Electrical and Computer Engineering. 2018 Dec;8(1):379-89.
[144] Gaurav K, Ghanekar U. Image steganography based on Canny edge detection, dilation operator and hybrid coding. J of Information Security and Applications. 2018 Aug;41:41-51.
[145] Sur A, Sagar SS, Pal R, Mitra P, Mukhopadhyay J. A new image watermarking scheme using saliency based visual attention model. In: Annual IEEE India Conference. Gujarat, India; 2009. p. 1-4.
[146] Basu A, Sarkar SK. On the implementation of robust copyright protection scheme using visual attention model. Information Security J: A Global Perspective. 2013 Jan;22(1):10-20.
[147] Nayak MR, Tudu B, Basu A, Sarkar SK. On the implementation of a secured digital watermarking framework. Information Security J: A Global Perspective. 2015 Dec;24(4-6):118-26.
[148] Itti L, Koch C, Niebur E. A model of saliency-based visual attention for rapid scene analysis. IEEE Trans on Pattern Analysis and Machine Intelligence. 1998 Nov;20(11):1254-9.
[149] Li C, Wang Y, Ma B, Zhang Z. Tamper detection and self-recovery of biometric images using salient region-based authentication watermarking scheme. Computer Standards and Interfaces. 2012 Jun;34(4):367-79.
[150] Harel J, Koch C, Perona P. Graph-based visual saliency. In: Int. Conf. on Neural Information Processing Systems. Cambridge, MA, USA; 2006. p. 545–552.
[151] Erdem E, Erdem A. Visual saliency estimation by nonlinearly integrating features using region covariances. J of Vision. 2013 Mar;13(4):11.
[152] Sajjad M, Muhammad K, Baik SW, Rho S, Jan Z, Yeo SS, et al. Mobile-cloud assisted framework for selective encryption of medical images with steganography for resource-constrained devices. Multimedia Tools and Applications. 2017 Feb;76(3):3519-36.
[153] Liu Y, Qu X, Xin G. A ROI-based reversible data hiding scheme in encrypted medical images. J of Visual Communication and Image Representation. 2016 Aug;39:51-7.
[154] Khor HL, Liew SC, Zain JM. Region of interest-based tamper detection and lossless recovery watermarking scheme (ROI-DR) on ultrasound medical images. J of Digital Imaging. 2017 Jun;30(3):328-49.
[155] Upham D. Jpeg-Jsteg source code; 1993. Available from: http://www.nic.funet.fi/pub/crypt/steganography/jpeg-jsteg-v4.diff.gz.
[156] Westfeld A. F5 — A steganographic algorithm. In: Int. Workshop on Information Hiding. Pittsburgh, PA, USA; 2001. p. 289-302.
[157] Jaheel HL, Beiji Z, Jaheel AL. Design and implementation steganography system by using visible image. Int J on Smart Sensing and Intelligent Systems. 2015 Jun;8(2):1011-30.
[158] Liu CL, Liao SR. High-performance JPEG steganography using complementary embedding strategy. Pattern Recognition. 2008 Sep;41(9):2945-55.
[159] Li X, Wang J. A steganographic method based upon JPEG and particle swarm optimization algorithm. Information Sciences. 2007 Aug;177(15):3099-109.
[160] Aslantas V, Ozer S, Ozturk S. Improving the performance of DCT-based fragile watermarking using intelligent optimization algorithms. Optics Communications. 2009 Jul;282(14):2806-17.
[161] Ejaz N, Anwar J, Ishtiaq M, Baik SW. Adaptive image data hiding using transformation and error replacement. Multimedia Tools and Applications. 2014 Nov;73(2):825-40.
[162] Sarmah DK, Kulkarni AJ. JPEG based steganography methods using cohort intelligence with cognitive computing and modified multi random start local search optimization algorithms. Information Sciences. 2018 Mar;430-431:378-96.
[163] Sarmah DK, Kulkarni AJ. Improved cohort intelligence - A high capacity, swift and secure approach on JPEG image steganography. J of Information Security and Applications. 2019 Apr;45:90-106.
[164] Fridrich J, Goljan M, Du R. Lossless data embedding - New paradigm in digital watermarking. EURASIP J on Applied Signal Processing. 2002 Dec;2002(2):185-96.
[165] Kim S, Huang F, Kim HJ. Reversible data hiding in JPEG images using quantized DC. Entropy. 2019 Sep;21(9):835.
[166] Singh RK, Shaw DK. A hybrid concept of cryptography and dual watermarking (LSB_DCT) for data security. Int J of Information Security and Privacy. 2018 Jan;12(1):1-12.
[167] Tauhid A, Tasnim M, Noor SA, Faruqui N, Yousuf MA. A secure image steganography using advanced encryption standard and discrete cosine transform. J of Information Security. 2019 Jun;10(3):117-29.
[168] Hsu CT, Wu JL. Hidden digital watermarks in images. IEEE Trans on Image Processing. 1999 Jan;8(1):58-68.
[169] Kobayashi H, Noguchi Y, Kiya H. A method of embedding binary data into JPEG bitstreams. Systems and Computers in Japan. 2002;33(1):18-26.

[170] Tseng HW, Chang CC. High capacity data hiding in JPEG-compressed images. Informatica. 2004;15(1):127-42.
[171] Tian J. Reversible data embedding using a difference expansion. IEEE Trans on Circuits and Systems for Video Technology. 2003 Aug;13(8):890-6.
[172] Alattar AM. Reversible watermark using the difference expansion of a generalized integer transform. IEEE Trans on Image Processing. 2004 Aug;13(8):1147-56.
[173] Lee CC, Wu HC, Tsai CS, Chu YP. Adaptive lossless steganographic scheme with centralized difference expansion. Pattern Recognition. 2008 Jun;41(6):2097-106.
[174] Chen CC, Tsai YH. Adaptive reversible image watermarking scheme. J of Systems and Software. 2011 Mar;84(3):428-34.
[175] Thodi DM, Rodriguez JJ. Expansion embedding techniques for reversible watermarking. IEEE Trans on Image Processing. 2007 Mar;16(3):721-30.
[176] Coltuc D. Improved embedding for prediction-based reversible watermarking. IEEE Trans on Information Forensics and Security. 2011 Sep;6(3):873-82.
[177] Coltuc D. Low distortion transform for reversible watermarking. IEEE Trans on Image Processing. 2012 Jan;21(1):412-7.
[178] Coltuc D, Chassery JM. Very fast watermarking by reversible contrast mapping. IEEE Signal Processing Letters. 2007 Apr;14(4):255-8.
[179] Maity SP, Maity HK. On adaptive distortion control in reversible watermarking using modified reversible contrast mapping. Multimedia Tools and Applications. 2016 Jul;75(13):7931-56.
[180] Said A, Pearlman WA. An image multiresolution representation for lossless and lossy compression. IEEE Trans on Image Processing. 1996 Sep;5(9):1303-10.
[181] Lee S, Yoo CD, Kalker T. Reversible image watermarking based on integer-to-integer wavelet transform. IEEE Trans on Information Forensics and Security. 2007 Sep;2(3):321-30.
[182] Ghebleh M, Kanso A. A robust chaotic algorithm for digital image steganography. Communications in Nonlinear Science and Numerical Simulation. 2014 Jun;19(6):1898-907.
[183] Sweldens W. The lifting scheme: A custom-design construction of biorthogonal wavelets. Applied and Computational Harmonic Analysis. 1996 Apr;3(2):186-200.
[184] Liu XL, Lin CC, Yuan SM. Blind dual watermarking for color images' authentication and copyright protection. IEEE Trans on Circuits and Systems for Video Technology. 2018 May;28(5):1047-55.
[185] Bhattacharyya D, Dutta J, Das P, Bandyopadhyay R, Bandyopadhyay SK, Kim TH. Discrete Fourier transformation based image authentication technique. In: Proc. IEEE Int. Conf. on Cognitive Informatics. Hong Kong, China; 2009. p. 196-200.
[186] Mandal JK, Khamrui A. A genetic algorithm based steganography in frequency domain (GASFD). In: Int. Conf. on Communication and Industrial Applications. Kolkata, India; 2011. p. 1-4.
[187] Sharma D, Saxena R, Singh N. Dual domain robust watermarking scheme using random DFRFT and least significant bit technique. Multimedia Tools and Applications. 2017 Feb;76(3):3921-42.
[188] Fridrich J, Goljan M, Hogea D. New methodology for breaking steganographic techniques for JPEGs. In: SPIE Electronic Imaging. Santa Clara, CA, USA; 2003. p. 143-55.
[189] Le PQ, Dong F, Hirota K. A flexible representation of quantum images for polynomial preparation, image compression, and processing operations. Quantum Information Processing. 2011 Feb;10(1):63-84.
[190] Zhang Y, Lu K, Gao Y, Wang M. NEQR: A novel enhanced quantum representation of digital images. Quantum Information Processing. 2013 Aug;12(8):2833-60.
[191] Jiang N, Zhao N, Wang L. LSB based quantum image steganography algorithm. Int J of Theoretical Physics. 2016 Jan;55(1):107-23.
[192] Heidari S, Naseri M. A novel LSB based quantum watermarking. Int J of Theoretical Physics. 2016 Oct;55(10):4205-18.
[193] Zhou RG, Hu W, Fan P. Quantum watermarking scheme through Arnold scrambling and LSB steganography. Quantum Information Processing. 2017 Jul;16(9):212:1-21.
[194] Li P, Lu A. LSB-based steganography using reflected Gray code for color quantum images. Int J of Theoretical Physics. 2018 May;57(5):1516-48.
[195] Miyake S, Nakamae K. A quantum watermarking scheme using simple and small-scale quantum circuits. Quantum Information Processing. 2016 May;15(5):1849-64.
[196] Li P, Zhao Y, Xiao H, Cao M. An improved quantum watermarking scheme using small-scale quantum circuits and color scrambling. Quantum Information Processing. 2017 May;16(5):1-34.
[197] Naseri M, Heidari S, Baghfalaki M, Fatahi N, Gheibi R, Batle J, et al. A new secure quantum watermarking scheme. Optik. 2017 Jun;139:77-86.
[198] Zhou RG, Luo J, Liu X, Zhu C, Wei L, Zhang X. A novel quantum image steganography scheme based on LSB. Int J of Theoretical Physics. 2018 Jun;57(6):1848-63.
[199] Heidari S, Farzadnia E. A novel quantum LSB-based steganography method using the Gray code for colored quantum images. Quantum Information Processing. 2017 Aug;16(10):242.
[200] Luo G, Zhou RG, Mao Y. Two-level information hiding for quantum images using optimal LSB. Quantum Information Processing. 2019 Aug;18(10):297.
[201] Hu W, Zhou RG, Luo J, Liu B. LSBs-based quantum color images watermarking algorithm in edge region. Quantum Information Processing. 2018 Nov;18(1):16.
[202] Hu W, Zhou RG, Li Y. Quantum watermarking based on neighbor mean interpolation and LSB steganography algorithms. Int J of Theoretical Physics. 2019 Jul;58(7):2134-57.
[203] Luo G, Zhou RG, Luo J, Hu W, Zhou Y, Ian H. Adaptive LSB quantum watermarking method using tri-way pixel value differencing. Quantum Information Processing. 2019 Jan;18(2):49.

[204] Vatsa M, Singh R, Noore A, Houck MM, Morris K. Robust biometric image watermarking for fingerprint and face template protection. IEICE Electronics Express. 2006 Jan;3(2):23-8.
[205] Low CY, Teoh ABJ, Tee C. Fusion of LSB and DWT biometric watermarking using offline handwritten signature for copyright protection. In: Int. Conf. on Advances in Biometrics. Alghero, Italy; 2009. p. 786-95.
[206] Kamal AHM, Islam MM. Facilitating and securing offline e-medicine service through image steganography. Healthcare Technology Letters. 2014;1(2):74-9.
[207] Karakis R, Güler I, Capraz I, Bilir E. A novel fuzzy logic-based image steganography method to ensure medical data security. Computers in Biology and Medicine. 2015 Dec;67:172-83.
[208] Muhammad K, Sajjad M, Baik SW. Dual-level security based Cyclic18 steganographic method and its application for secure transmission of keyframes during wireless capsule endoscopy. J of Medical Systems. 2016 Mar;40(5):114.
[209] Sajedi H. Applications of data hiding techniques in medical and healthcare systems: A survey. Network Modeling Analysis in Health Informatics and Bioinformatics. 2018 Apr;7(1):6.
[210] Das R, Chatterjee P. Securing data transfer in IoT employing an integrated approach of cryptography and steganography. In: Int. Conf. on High Performance Compilation, Computing and Communications. New York, NY, USA; 2017. p. 17-22.
[211] Yang W, Wang S, Hu J, Ibrahim A, Zheng G, Macedo MJ, et al. A cancelable iris- and steganography-based user authentication system for the internet of things. Sensors. 2019 Jul;19(13):2985.
[212] Janakiraman S, Thenmozhi K, Rayappan JBB, Amirtharajan R. Indicator-based lightweight steganography on 32-bit RISC architectures for IoT security. Multimedia Tools and Applications. 2019 Jul;78(22):31485–31513.
[213] Muhammad K, Ahmad J, Rho S, Baik SW. Image steganography for authenticity of visual contents in social networks. Multimedia Tools and Applications. 2017 Sep;76(18):18985-9004.
[214] Muhammad K, Sajjad M, Mehmood I, Rho S, Baik SW. Image steganography using uncorrelated color space and its application for security of visual contents in online social networks. Future Generation Computer Systems. 2018 Sep;86:951-60.
[215] Lee HY, Im DH, Lee HK. Error concealment technique of satellite imagery transmission through information hiding. IEICE Trans on Information and Systems. 2007 Nov;E90-D(11):1881-4.
[216] Rodriguez MJ, Leyferman CEP, Gutierrez JCE, Novoa MGG, Rodriguez HG, Siordia OF. Steganography applied in the origin claim of pictures captured by drones based on chaos. Ingenieria e Investigacion. 2018 May;38(2):61-9.
[217] Rura L, Issac B, Haldar MK. Secure electronic voting system based on image steganography. In: IEEE Conf. on Open Systems. Langkawi, Malaysia; 2011. p. 80-5.
[218] Yuan L, Li M, Guo C, Hu W, Tan X. A verifiable e-voting scheme with secret sharing. In: IEEE Int. Conf. on Communication Technology. Hangzhou, China; 2015. p. 304-8.
[219] Garg M, Gupta S, Khatri P. Fingerprint watermarking and steganography for ATM transaction using LSB-RSA and 3-DWT algorithm. In: Int. Conf. on Communication Networks. Gwalior, India; 2015. p. 246-51.
[220] Bucerzan D, Rațiu C, Manolescu MJ. SmartSteg: A new Android based steganography application. Int J of Computers Communications & Control. 2013 Sep;8(5):681-8.
[221] Pelosi MJ, Poudel N, Lamichhane P, Soomro DB. Steganography system with application to cryptocurrency cold storage and secure transfer. Advances in Science Technology and Engineering Systems. 2018 Apr;3(2):271-82.
[222] Pelosi MJ. OTP-Steg; 2015. Available from: http://www.mauisolarsoftware.com/OTP-Steg/.
[223] Celik MU, Sharma G, Tekalp AM, Saber E. Reversible data hiding. In: Int. Conf. on Image Processing. Rochester, NY, USA; 2002. p. II-157160.
[224] Hanafy AA, Salama GI, Mohasseb YZ. A secure covert communication model based on video steganography. In: IEEE Military Communications Conference. San Diego, CA, USA; 2008. p. 1-6.
[225] Younus ZS, Younus GT. Video steganography using knight tour algorithm and LSB method for encrypted data. J of Intelligent Systems. 2019 Feb;29(1):1216-25.
[226] Lin SS, Wei CL. Optimal algorithms for constructing knight's tours on arbitrary n × m chessboards. Discrete Applied Mathematics. 2005 Mar;146(3):219-32.
[227] Eltahir ME, Kiah LM, Zaidan BB, Zaidan AA. High rate video streaming steganography. In: Int. Conf. on Future Computer and Communication. Kuala Lumpur, Malaysia; 2009. p. 672-5.
[228] Dasgupta K, Mondal JK, Dutta P. Optimized video steganography using genetic algorithm (GA). Procedia Technology. 2013 Dec;10:131-7.
[229] Mstafa RJ, Elleithy KM. A highly secure video steganography using Hamming code (7, 4). In: Long Island Systems, Applications and Technology Conference. Farmingdale, NY, USA; 2014. p. 1-6.
[230] Manisha S, Sharmila TS. A two-level secure data hiding algorithm for video steganography. Multidimensional Systems and Signal Processing. 2019 Apr;30(2):529-42.
[231] Guo L, Ni J, Shi YQ. Uniform embedding for efficient JPEG steganography. IEEE Trans on Information Forensics and Security. 2014 May;9(5):814-25.
[232] Ramalingam M, Isa NAM. Video steganography based on integer Haar wavelet transforms for secured data transfer. Indian J of Science and Technology. 2014 Jul;7(7):897-904.
[233] Mstafa RJ, Elleithy KM. A high payload video steganography algorithm in DWT domain based on BCH codes (15, 11). In: Wireless Telecommunication Symposium. New York, NY, USA; 2015. p. 1-8.
[234] Mobasseri BG, Evans AT. Content-dependent video authentication by self-watermarking in color space. In: SPIE Photonics West - Electronic Imaging. San Jose, CA, USA; 2001. p. 35-44.

[235] Arab F, Abdullah SM, Hashim SZM, Manaf AA, Zamani M. A robust video watermarking technique for the tamper detection of surveillance systems. Multimedia Tools and Applications. 2016 Sep;75(18):10855-85.
[236] Tong M, Guo J, Tao S, Wu Y. Independent detection and self-recovery video authentication mechanism using extended NMF with different sparseness constraints. Multimedia Tools and Applications. 2016 Jul;75(13):8045-69.
[237] Amanipour V, Ghaemmaghami S. Video-tampering detection and content reconstruction via self-embedding. IEEE Trans on Instrumentation and Measurement. 2018 Mar;67(3):505-15.
[238] Shi Y, Qi M, Yi Y, Zhang M, Kong J. Object based dual watermarking for video authentication. Optik. 2013 Oct;124(19):3827-34.
[239] Celik MU, Sharma G, Tekalp AM, Saber ES. Video authentication with self-recovery. In: SPIE Electronic Imaging. San Jose, CA, USA; 2002. p. 531-41.
[240] Mstafa RJ, Elleithy KM. A new video steganography algorithm based on the multiple object tracking and Hamming codes. In: IEEE Int. Conf. on Machine Learning and Applications. Miami, FL, USA; 2015. p. 335-40.
[241] Mstafa RJ, Elleithy KM. A video steganography algorithm based on Kanade-Lucas-Tomasi tracking algorithm and error correcting codes. Multimedia Tools and Applications. 2016 Sep;75(17):10311-33.
[242] Mstafa RJ, Elleithy KM, Abdelfattah E. A robust and secure video steganography method in DWT-DCT domains based on multiple object tracking and ECC. IEEE Access. 2017 Apr;5:5354-65.
[243] Wang J, Jia X, Kang X, Shi YQ. A cover selection HEVC video steganography based on intra prediction mode. IEEE Access. 2019 Sep;7:119393-402.
[244] Zhang H, Cao Y, Zhao X. Motion vector-based video steganography with preserved local optimality. Multimedia Tools and Applications. 2016 Nov;75(21):13503-19.
[245] Westfeld A, Wolf G. Steganography in a video conferencing system. In: Int. Workshop on Information Hiding. Portland, OR, USA; 1998. p. 32-47.
[246] Robie DL, Mersereau RM. Video error correction using steganography. EURASIP J on Advances in Signal Processing. 2002 Feb;2002(2):164-73.
[247] Swati S, Hayat K, Shahid Z. A watermarking scheme for high efficiency video coding (HEVC). PLoS ONE. 2014 Aug;9(8):e105613:1-8.
[248] Shahid Z, Chaumont M, Puech W. Considering the reconstruction loop for data hiding of intra- and inter-frames of H.264/AVC. Signal, Image and Video Processing. 2013 Jan;7(1):75-93.
[249] Xu D, Wang R, Wang J. Prediction mode modulated data-hiding algorithm for H.264/AVC. J of Real-Time Image Processing. 2012 Dec;7(4):205-14.
[250] Liu S, Rho S, Jifara W, Jiang F, Liu C. A hybrid framework of data hiding and encryption in H.264/SVC. Discrete Applied Mathematics. 2018 May;241:48-57.
[251] Zhang J, Li J, Zhang L. Video watermark technique in motion vector. In: Brazilian Symp. on Computer Graphics and Image Processing. Florianpolis, Brazil; 2001. p. 179-82.
[252] Aly HA. Data hiding in motion vectors of compressed video based on their associated prediction error. IEEE Trans on Information Forensics and Security. 2011 Mar;6(1):14-8.
[253] Cao Y, Zhang H, Zhao X, Yu H. Covert communication by compressed videos exploiting the uncertainty of motion estimation. IEEE Communication Letters. 2015 Feb;19(2):203-6.
[254] Yao Y, Zhang W, Yu N, Zhao X. Defining embedding distortion for motion vector-based video steganography. Multimedia Tools and Applications. 2015 Dec;74(24):11163-86.
[255] Langelaar GC, Lagendijk RL, Biemond J. Real-time labeling of MPEG-2 compressed video. J of Visual Communication and Image Representation. 1998 Dec;9(4):256-70.
[256] Seo YH, Choi HJ, Lee CY, Kim DW. Low-complexity watermarking based on entropy coding in H.264/AVC. IEICE Trans on Fundamentals of Electronics Communications and Computer Sciences. 2008 Aug;E91-A(8):2130-7.
[257] Wang K, Zhao H, Wang H. Video steganalysis against motion vector-based steganography by adding or subtracting one motion vector value. IEEE Trans on Information Forensics and Security. 2014 May;9(5):741-51.
[258] Ren Y, Zhai L, Wang L, Zhu T. Video steganalysis based on subtractive probability of optimal matching feature. In: ACM Workshop on Information Hiding and Multimedia Security. Salzburg, Austria; 2014. p. 83-90.
[259] Su Y, Zhang C, Zhang C. A video steganalytic algorithm against motion-vector-based steganography. Signal Processing. 2011 Aug;91(8):1901-9.
[260] Cao Y, Zhao X, Feng D. Video steganalysis exploiting motion vector reversion-based features. IEEE Signal Processing Letters. 2012 Jan;19(1):35-8.
[261] Zhang W, Cheung SS, Chen M. Hiding privacy information in video surveillance system. In: IEEE Int. Conf. on Image Processing. Genova, Italy; 2005. p. II-868.
[262] Zhang YJ, Zhang YY. Design and implementation of video copyright protection system based on LabVIEW and water transfer printing materials. Advanced Materials Research. 2012 Feb;460:206-9.
[263] Carvalho DF, Chies R, Freire AP, Martimiano LAF, Goularte R. Video steganography for confidential documents: Integrity, privacy and version control. In: Annual ACM Int. Conf. on Design of Communication. Lisbon, Portugal; 2008. p. 199-206.
[264] Lie WN, Lin TCI, Lin CW. Enhancing video error resilience by using data-embedding techniques. IEEE Trans on Circuits and Systems for Video Technology. 2006 Feb;16(2):300-8.
[265] Zhou H, Chen K, Zhang W, Yao Y, Yu N. Distortion design for secure adaptive 3-D mesh steganography. IEEE Trans on Multimedia. 2019 Jun;21(6):1384-98.
[266] Wu HT, Dugelay JL. Steganography in 3D geometries and images by adjacent bin mapping. EURASIP J on Information Security. 2009 Dec;2009(1):1-10.

[267] Wu HT, Dugelay JL, Cheung YM. A data mapping method for steganography and its application to images. In: Int. Workshop on Information Hiding. Santa Barbara, CA, USA; 2008. p. 236-50.
[268] Thiyagarajan P, Natarajan V, Aghila G, Venkatesan VP, Anitha R. Pattern based 3D image steganography. 3D Research. 2013 Apr;4(1):1.
[269] Jiang R, Zhou H, Zhang W, Yu N. Reversible data hiding in encrypted three-dimensional mesh models. IEEE Trans on Multimedia. 2018 Jan;20(1):55-67.
[270] Gallager R. Low-density parity-check codes. IRE Transactions on Information Theory. 1962 Jan;8(1):21-8.
[271] Golay MJE. Notes on digital coding. Proceedings of the IEEE. 1949 Jun;37:657.
[272] Yang Y, Peyerimhoff N, Ivrissimtzis I. Linear correlations between spatial and normal noise in triangle meshes. IEEE Trans on Visualization and Computer Graphics. 2013 Jan;19(1):45-55.
[273] The Stanford 3D scanning repository; 2014. Available from: http://graphics.stanford.edu/data/3Dscanrep/.
[274] Shilane P, Min P, Kazhdan M, Funkhouser T. The Princeton Shape Benchmark. In: Shape Modeling International. Genova, Italy; 2004. p. 167-78.
[275] Yang Y, Ivrissimtzis I. Mesh discriminative features for 3D steganalysis. ACM Trans on Multimedia Computing, Communications, and Applications. 2014 Apr;10(3):1-13.
[276] Rugis J, Klette R. A scale invariant surface curvature estimator. In: Pacific-Rim Symposium on Image and Video Technology. Hsinchu, Taiwan; 2006. p. 138-47.
[277] Jin JQ, Dai MY, Bao JJ, Peng QS. Watermarking on 3D mesh based on spherical wavelet transform. J of Zhejiang University-SCIENCE A. 2004 Mar;5(3):251-8.
[278] Luo T, Jiang G, Wang X, Yu M, Shao F, Peng Z. Stereo image watermarking scheme for authentication with self-recovery capability using inter-view reference sharing. Multimedia Tools and Applications. 2014 Dec;73(3):1077-102.
[279] Luo T, Jiang G, Yu M, Xu H. Asymmetric self-recovery oriented stereo image watermarking method for three dimensional video system. Multimedia Systems. 2016 Oct;22(5):641-55.
[280] Yang WC, Chen LH. Reversible DCT-based data hiding in stereo images. Multimedia Tools and Applications. 2015 Sep;74(17):7181-93.
[281] Dhaou D, Jabra SB, Zagrouba E. An efficient anaglyph 3D video watermarking approach based on hybrid insertion. In: Int. Conf. on Computer Analysis of Images and Patterns. Salerno, Italy; 2019. p. 96-107.
[282] Dhaou D, Jabra SB, Zagrouba E. A multi-sprite based anaglyph 3D video watermarking approach robust against collusion. 3D Research. 2019 Jun;10(2):1-15.
[283] Tran DN, Zepernick HJ. Spherical light-weight data hiding in 360-degree videos with equirectangular projection. In: Int. Conf. on Advanced Technologies for Communication. Hanoi, Vietnam; 2019. p. 56-62.
[284] Tran DN, Zepernick HJ. Spherical LSB data hiding in 360° videos using morphological operations. In: Int. Conf. on Signal Processing and Communication Systems. Gold Coast, QLD, Australia; 2019. p. 573-82.
[285] Tran DN, Zepernick HJ, Chu TMC. Viewing direction based LSB data hiding in 360° Videos. Electronics. 2021 Jun;10(1527):1-32.
[286] Yershov A, Zabiniako V, Semenchuk P. Using concatenated steganography for visual analysis in GIS SOA. Applied Computer Systems. 2012 Nov;13(1):74-82.
[287] Zhang W, Cheung S, Chen M. Hiding privacy information in video surveillance system. In: IEEE Int. Conf. on Image Processing. Genova, Italy; 2005. p. II-868.
[288] Paruchuri JK, Cheung SS, Hail MW. Video data hiding for managing privacy information in surveillance systems. EURASIP J on Information Security. 2009 Sep;2009:1-18.
[289] Chaudhary S, Berki E, Nykänen P, Zolotavkin Y, Helenius M, Kela J. Towards a conceptual framework for privacy protection in the use of interactive 360° video surveillance. In: Int. Conf. on Virtual System Multimedia. Kuala Lumpur, Malaysia; 2016. p. 1-10.
[290] Ali A, Saad AHS, Ismael AH. VRNFC-Stego: Data hiding technique based on VR images and NFC-enabled smartphones. Procedia Computer Science. 2020 Jan;171:1551-60.
[291] Miura Y, Li X, Kang S, Sakamoto Y. Data hiding technique for omnidirectional JPEG images displayed on VR spaces. In: Int. Workshop on Advanced Image Technology. Chiang Mai, Thailand; 2018. p. 1-4.