Multimed Tools Appl (2017) 76:21749–21786
DOI 10.1007/s11042-016-4055-1

Compressed and raw video steganography techniques: a comprehensive survey and analysis

Ramadhan J. Mstafa[1] **· Khaled M. Elleithy**[1]

Received: 11 April 2016 / Revised: 28 September 2016 / Accepted: 6 October 2016 /
Published online: 9 November 2016

Abstract In the last two decades, the science of covertly concealing and communicating data has acquired tremendous significance due to the technological advancement in communication and digital content. Steganography is the art of concealing secret data in a particular interactive media transporter, e.g., text, audio, image, and video data in order to build a covert communication between authorized parties. Nowadays, video steganography techniques have become important in many video-sharing and social networking applications such as Livestreaming, YouTube, Twitter, and Facebook because of the noteworthy development of advanced video over the Internet. The performance of any steganographic method ultimately relies on the imperceptibility, hiding capacity, and robustness. In the past decade, many video steganography methods have been proposed; however, the literature lacks of sufficient survey articles that discuss all techniques. This paper presents a comprehensive study and analysis of numerous cutting edge video steganography methods and their performance evaluations from literature. Both compressed and raw video steganography methods are surveyed. In the compressed domain, video steganography techniques are categorized according to the video compression stages as venues for data hiding such as intra frame prediction, inter frame prediction, motion vectors, transformed and quantized coefficients, and entropy coding. On the other hand, raw video steganography methods are classified into spatial and transform domains. This survey suggests current research directions and recommendations to improve on existing video steganography techniques.

Keywords Video steganography · Compressed domain · Raw domain · Video processing · Smart video transmission · Smart video tracking · Imperceptibility · Hiding capacity

✉ Ramadhan J. Mstafa
rmstafa@my.bridgeport.edu

Khaled M. Elleithy
elleithy@bridgeport.edu

[1] Department of Computer Science and Engineering, University of Bridgeport, Bridgeport, CT 06604, USA

1 Introduction

In spite of the fact that the Internet is utilized as well-known venues for users to access desired data, it has likewise opened another entryway for attackers to obtain precious and intellectual information of other users with little exertion [11]. Steganography has functioned in a complementary capacity to offer a protection mechanism that prevents eavesdroppers from any ongoing communication between an authorized transmitter and its recipient [23]. Steganography is characterized as the art of concealing secret information in specific carrier data, establishing covert communication channels between official parties [105]. Subsequently, a stego object (steganogram) should be same as an original data that has the same statistical features. Carrier data is also referred as cover or host data [61, 84]. Carriers can be acknowledged in various forms such as text, audio, image, and video. A hidden message can also appear in any form of data such as such as text, audio, image, and video [24, 59]. The primary objective of steganography is to remove any hacker's suspicion to the transmission of hidden messages and provide security and anonymity for legitimate parties. Simple way to observe the steganogram visual quality is to determine its accuracy which is achieved through the human visual system (HVS). The HVS cannot identify slight distortions in steganogram, thus avoiding suspiciousness [97]. However, if the size of the hidden message in proportion with the size of the carrier object is large, then the steganogram's degradation will be visible to the human eye resulting in a failed steganographic method [34]. Figure 1 represents the general model of steganographic method.

Embedding efficiency, hiding capacity, and robustness are the three major requirements incorporated in any successful steganographic methods [19, 26]. First, embedding efficiency can be determined by answering the following questions [68, 83]: 1) How safe is the steganographic method to conceal the hidden information inside the carrier object? 2) How precise are the steganograms' qualities after the hiding procedure happens? and 3) Is the secret message undetectable from the steganogram? In other words, the steganographic method is highly efficient if it includes encryption, imperceptibility, and undetectability characteristics. The high efficient algorithm conceals the covert information into the carrier data by utilizing

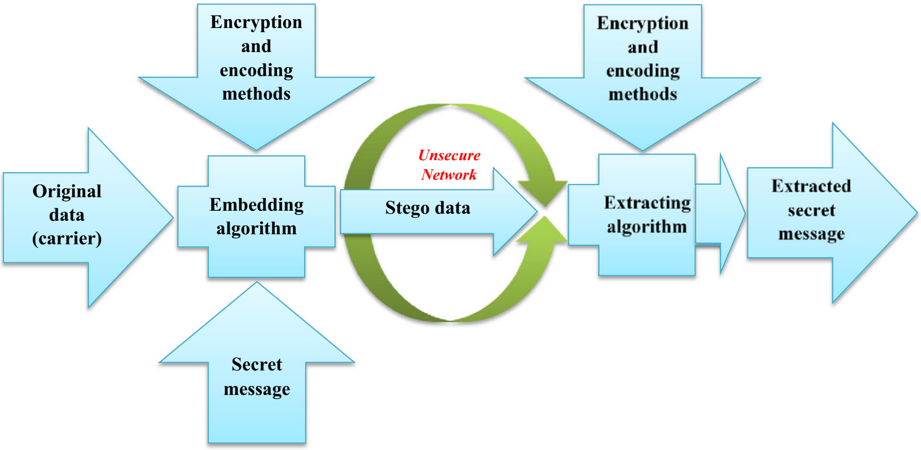


Fig. 1 General diagram of the steganography method

some of the encoding and encryption techniques prior to the embedding process to enhance the security of the algorithm [22, 90].

Obtained steganograms with low alteration rate and high quality do not draw the hacker's attention, and thus will avoid any suspicion to the sending of covert information. If the steganography method is more effective, then the steganalytical detectors will find it more challenging to detect the hidden message [21, 89].

The hiding capacity is the second fundamental requirement which permits any steganography method to expand the size of hidden message taking into account the visual quality of steganograms. The hiding capacity is the quantity of the covert messages needed to be inserted inside the carrier object. In ordinary steganographic methods, both hiding capacity and embedding efficiency are contradictory [13, 90]. Conversely, if the hiding capacity is expanded, then the quality of steganograms will be diminished which decreases the algorithm's efficiency. The embedding efficiency of the steganographic method is directly affected on its embedding payload. To expand the hiding capacity with the minimum alteration rate of the carrier object, many steganographic methods have been presented using different strategies. These methods utilize linear block codes and matrix encoding principles which include Bose, Chaudhuri, and Hocquenghem (BCH) codes, Hamming codes, cyclic codes, Reed-Solomon codes, and Reed-Muller codes [20, 113].

Robustness is the third requirement which calculates the steganographic method's strength against attacks and signal processing operations [42]. These operations contain geometrical transformation, compression, cropping, and filtering. A steganographic method is robust when the recipient obtains the hidden information accurately, without any flaws. High efficient steganography methods withstand against both adaptive noises and signal processing operations [69, 110]. Recently, a large number of video steganography techniques have been proposed in the literature. Unfortunately, the literature lacks of video steganography survey articles. Therefore, this leads to present an extensive study that includes all video steganography techniques for the past decade. This paper unlike others provides a comprehensive survey and analysis of the state-of-the-art video steganography methods in both compressed and raw domains. In addition, this survey not only investigates the existing video steganography techniques but also provides recommendations and future directions to enhance those methods. The remaining parts of the paper are organized as follows: Section 2 explains steganography versus cryptography and watermarking. A comprehensive study and analysis of the state-of-the-art video steganography methods in compressed and raw domains is given in 3. Section 4 presents some of well-known performance assessment metrics. Section 5 summarizes the key findings of this survey, advises some recommendations to improve the existing methods, and suggests future research directions.

2 Steganography versus cryptography and watermarking

The common objective of both steganography and cryptography is to provide confidentiality and protection of data. The steganography "protected writing" establishes a covert communication channel between legitimate parties; while the cryptography "secret writing" creates an overt communication channel [1]. In cryptography, the presence of the secret data is recognizable; however, its content becomes unintelligible to illegitimate parties. In order to increase additional levels of security, steganography and cryptography can operate together in one system [14, 63].

Table 1 Comparison of steganography, cryptography, and watermarking techniques

Description	Steganography	Cryptography	Watermarking
Goal achieved:	Communication channels are covert	Data content of communication channels are covert	Copyright protection exists
Goal failed:	Communication is detected	Plain-text is retrieved	Watermark is erased or exchanged
Common carrier file:	Text, audio, image, or video	Plain-text or image	Image or video
Secret information:	Any type of data	plain-text	watermark
Secret keys:	May exist	Must exist	May exist
Extraction phase:	Carrier data is unnecessary	Carrier data is unnecessary during deciphering process	Carrier data availability depends on the application
Output file:	Steganogram	Cryptogram	Watermarked object
Security level:	Depends on the embedding algorithms	Depends on the secret keys	Depends on the watermarking algorithms
Information transparency:	Invisible	Visible	Transparency depends on the application
Robustness level:	Against detection	Against deciphering	Robust watermarking, fragile watermarking, and semi-fragile watermarking
Common attacks:	Steganalysis	Cryptanalysis	Signal processing operations
Requirements:	Embedding efficiency, embedding payload, undetectability, and robustness	Robustness	Robust watermarking requires robustness while fragile and semi-fragile watermarking do not need robustness

Digital watermarking techniques use a preservation mechanism to protect the copyright ownership information from unauthorized users. This process is accomplished by concealing the watermark information into overt carrier data [40]. Like steganography, watermarking can be used in many different applications such as content authentication, digital fingerprints, broadcast monitoring, copyright protection, and intellectual property protection [28, 29, 40, 49, 87]. Different watermarking techniques can be found in the literature [4, 8, 33, 41, 48, 50, 51, 85, 88]. Table 1 shows the general similarities and differences between steganography, cryptography, and watermarking techniques.

3 Video steganography techniques

Due to the advancement of Internet and multimedia technologies, digital videos have become a popular choice for data hiding. The video data contains a massive amount of data redundancy which can be utilized for embedding secret data. Recently, there are many useful applications of video steganography techniques such as video error correcting [47, 70, 71, 86, 109], military services [81], bandwidth saving [67, 96], video surveillance [62, 72, 112], and medical video security [73, 74, 76]. Video steganography techniques are classified into compressed and uncompressed domains. Figure 2 clarifies the hierarchy of the overall system security including video steganography, which is the main focus of this survey.

3.1 Video steganography techniques in compressed domain

The H.264 standard has increased the efficiency of video compression when compared to the previous versions. Some new features of H.264 video codec include flexible macroblock ordering, quarter-pixel interpolation, intra prediction in intra frame, deblocking filtering post-processing, and multiple frames reference capability [52, 94, 106, 108]. Usually, H.264 codec comprises a number of group of pictures (GOP). Every GOP includes three types of frames: intra (I) frame, predicted (P) frame, and bidirectional (B) frame. During the video compression process, the motion estimation and compensation processes minimize the temporal

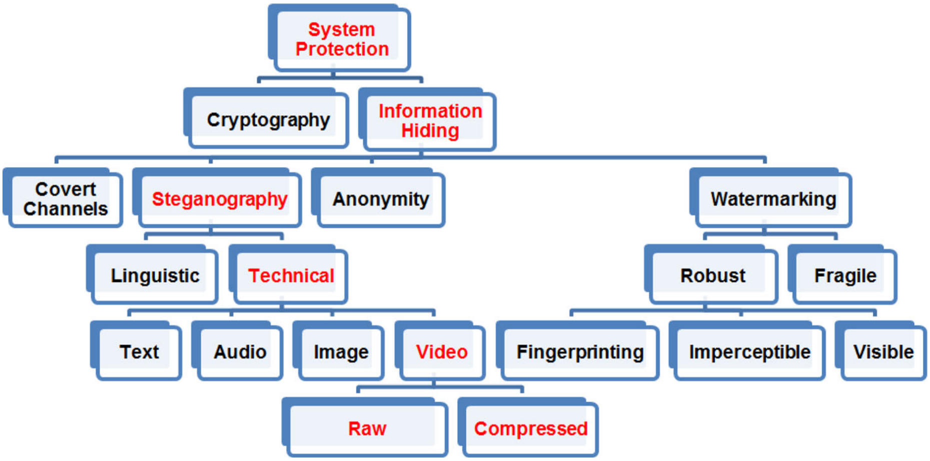


Fig. 2 Disciplines of overall system protection. The red color indicates the focus of this study

redundancy. Since the video stream is a number of correlated still images, a frame can be predicted by using one or more referenced frames based on the motion estimation and compensation techniques. First, frames are divided into 16 × 16 macroblocks (MB) wherein each MB contains blocks that may include the smallest size of 4 × 4. When applying a few searching algorithms, block C in the present frame is compared, individually, to one of the selected block $\widetilde{R}$ in the referenced frame $\widetilde{F}$ in order to find a corresponding block C. The prediction error between two blocks (C and $\widetilde{R}$) of size b can be measured using sum of absolute differences (SAD).

$$e = SAD\left(C, \tilde{R}\right) = \sum_{1 \le i,j \le b} \left| C_{i,j} - \tilde{r}_{i,j} \right| \tag{1}$$

Where $c_{i,j}$ *and* $\widetilde{r}_{i,j}$ refer to block values. The best matched block will have a minimum SAD using C's prediction denoted by $\widetilde{P}$. The motion vector (MV) and differential error $D = C - \widetilde{P}$ are required for the coding process. Video steganography techniques in compressed domain are categorized according to the video coding stages as venues for data hiding such as intra frame prediction, inter frame prediction, motion vectors, transformed and quantized coefficients, and entropy coding. Figure 3 illustrates the H.264 video codec standard indicating some venues for information hiding.

3.1.1 Video steganography techniques in intra frame prediction

During the video compression process, the macroblocks are encoded using a number of intra prediction modes. In H.264 codec, the numbers of intra prediction modes are nine of 4 × 4 blocks and four of 16 × 16 blocks which are illustrated in Fig. 4 and Fig. 5, respectively. Also, the high efficiency video coding (HEVC) codec can support up to 35 intra prediction modes

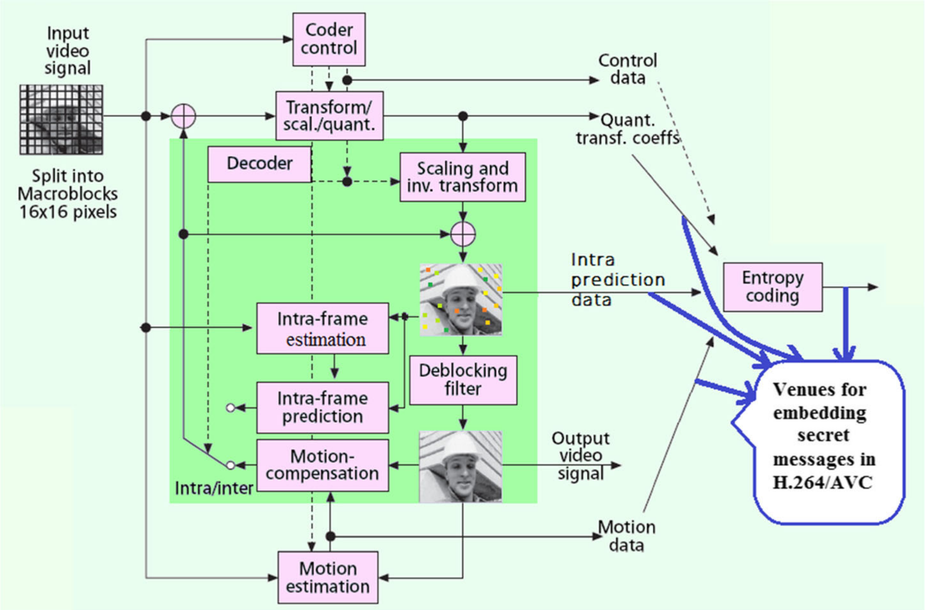


Fig. 3 H.264 hybrid video codec standard shows venues for data hiding

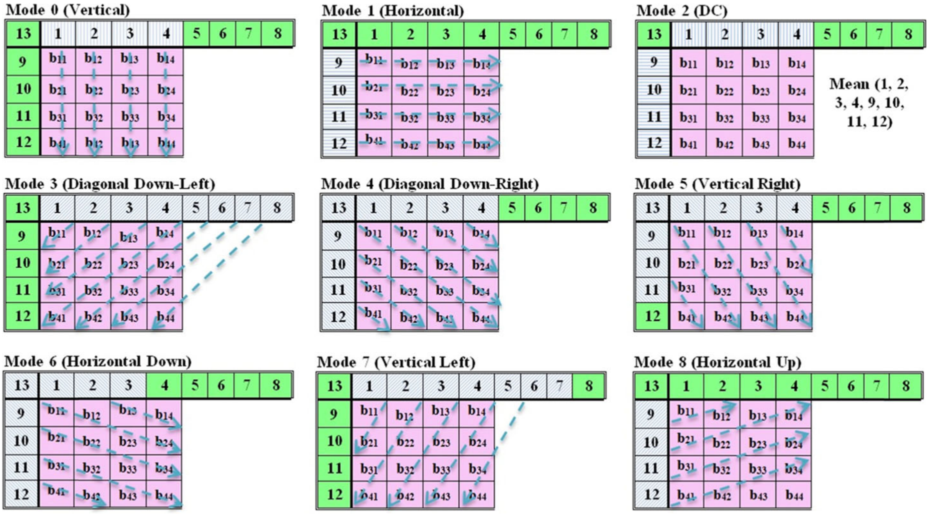


Fig. 4 H.264 intra prediction modes for 4 × 4 blocks

for each 64 × 64, 32 × 32, 16 × 16, 8 × 8, and 4 × 4 block sizes as shown in Fig. 6. For data concealing purposes, these modes can be mapped to one or more of secret message bits. Liu et al. [53] presented a new secure data hiding technique which performs entirely in a compressed domain. The framework of this algorithm consists of four stages. First, in the video sequences parser stage, the video sequences are coded, and discrete cosine transform (DCT) coefficients are obtained. In addition, the motion vectors, and the intra coded macroblocks are acquired. In the second stage, scene detection is performed on the consecutive intra frames to identify the fluctuation scenes. The fluctuation scene is identified using a histogram variation of DC coefficients within intra frame DCT coefficients. In the third stage, the embedding process is achieved using only intra frames of fluctuation scenes. The last stage is called video steganalysis. Here, the security level of the stego video is statistically measured to determine whether it is high or low. If the stego video cannot be passed by the steganalysis, then it will adjust the scale factor to make it stronger. The algorithm introduced by Liu et al. has limited capacity for hidden data because the fluctuation scenes of intra frames are only used for data embedding.

Chang et al. [9] presented a data concealing algorithm using HEVC utilizing both DCT and discrete sine transform (DST) methods. In this scheme, HEVC intra frames are used to conceal the hidden message without propagating the error of the distortion drift to the adjacent blocks. Blocks of quantized DCT and DST coefficients are selected for embedding the secret data by using a specific intra prediction mode. The combination modes of adjacent blocks will produce three directional patterns of error propagation for data hiding, consisting of vertical, horizontal,

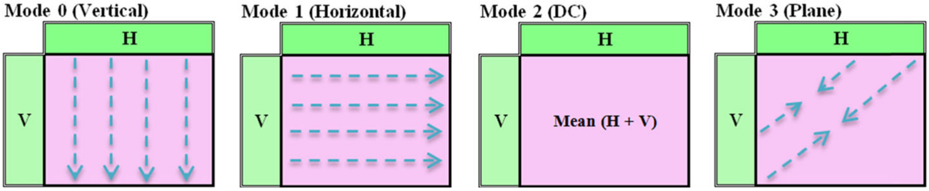


Fig. 5 H.264 intra prediction modes for 16 × 16 blocks

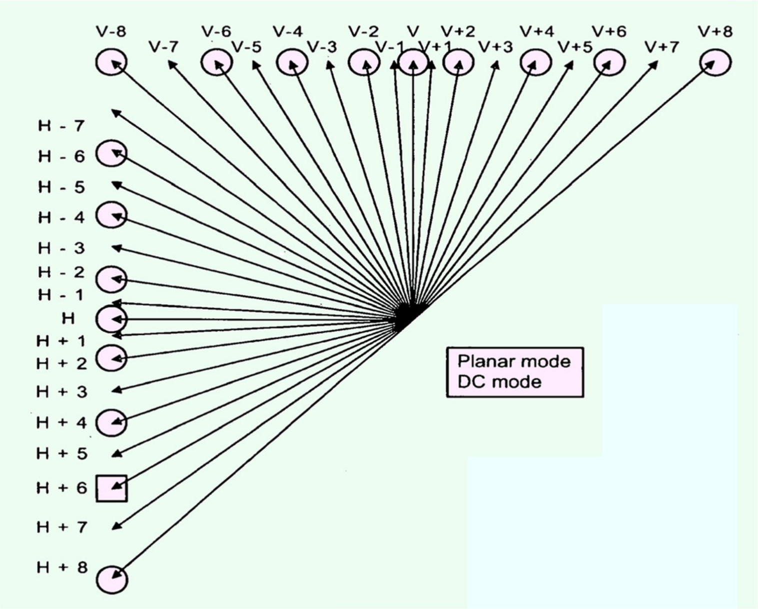


Fig. 6 The 35 HEVC intra prediction modes [111]

and diagonal. Each of the error propagation patterns has a range of intra prediction modes that protect a group of pixels in any particular direction. The range of the modes begin at 0 and ends at 34. Chang et al.'s algorithm lacks the embedding payload because the selection of blocks for the embedding process must meet certain conditions. Similarly, both Hu et al. [31] and Zhu et al. [115] presented data hiding methods using intra prediction modes for H.264/AVC. During the intra frame coding process, the secret message is embedded into the 4 × 4 luminance block. These algorithms utilize the 4 × 4 intra prediction modes in order to hide one bit of secret information per block. The 4 × 4 intra prediction modes are divided into two subsets based on the predefined mapping rules between the secret message and intra prediction modes in order to embed 0 or 1 of the secret message bits. Table 2 illustrates the mapping rule of 4 × 4 intra prediction modes of the Hu et al. method, which shows that each most probable mode and its candidate modes mapped to 0 or 1. Both Hu et al. and Zhu et al. methods achieve

Table 2 Mapping rules of 4 × 4 intra prediction modes [31]

Most Probable Mode	Candidate Modes Mapping to 0	Candidate Modes Mapping to 1
Mode 0	1, 2, 3, 4	5, 6, 7, 8
Mode 1	0, 3, 4, 8	2, 5, 6, 7
Mode 2	0, 3, 4, 8	1, 5, 6, 7
Mode 3	0, 5, 6, 8	1, 2, 4, 7
Mode 4	0, 3, 6, 8	1, 2, 5, 7
Mode 5	0, 3, 6, 8	1, 2, 4, 7
Mode 6	0, 3, 4, 8	1, 2, 5, 7
Mode 7	0, 5, 6, 8	1, 2, 3, 4
Mode 8	0, 1, 3, 4	2, 5, 6, 7

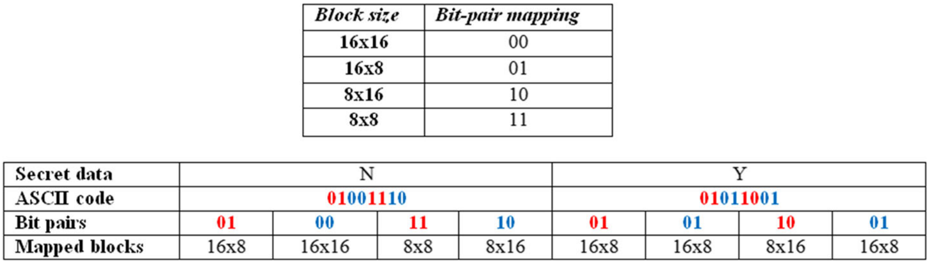
a negligible degradation of video quality as well as a small increase on the bit rate. In general, the steganographic techniques that use the intra frame prediction as venues for data hiding have low capacities to embed secret messages.

3.1.2 Video steganography techniques in inter frame prediction

In many video steganography methods, the seven block sizes that include 16x16, 16x8, 8x16, 8x8, 8x4, 4x8 and 4x4 of H.264 inter frame prediction are commonly utilized as a venue to embed the secret message by mapping each block type to a number of secret bits. Kapotas et al. [36] proposed a data concealing algorithm for scene change detection in H.264 coding. This method uses four different block sizes. Each one is mapped onto one pair of a secret message. In this algorithm, the secret message consists of scene change frames information that will be embedded into the encoded videos. This embedded information will help the scene change detection algorithm, in H.264 video stream, functioning in real time. However, the data hiding methods of the intra frame prediction have a very limited embedding capacity. For example, let "NY" is the secret information that must be embedded into the inter frame prediction blocks in H.264 codec. By using mapping rules of different block sizes the embedding goal can be achieved. Figure 7 illustrates the embedding process using mapping rules.

3.1.3 Video steganography techniques in motion vectors

Motion vector characteristics such as horizontal and vertical components, amplitude, and phase angles are utilized in embedding secret information. Xu et al. [107] proposed a compressed video stream steganography. In this scheme, the embedding process relies on I, P, and B frames. First, the hidden data is concealed into the motion vectors of, both, P and B frames. Only the motion vectors that have a high magnitude are chosen. Here, each macroblock has a motion vector; however, the selected macroblocks are moving rapidly. Secondly, the control information is embedded into I frames. This control information includes the capacity payload and segment range of each GOP. Each GOP contains one I frame which carries the control information necessary for the data extraction phase. In addition, each GOP has a number of P and B frames which contain secret messages in their high magnitude motion vectors. Xu et al.'s method has a low embedding payload because it only used the motion vectors with a high magnitude. Pan et al. [78] presented a new steganography method in the H.264 video standard based on the motion vectors and linear block codes. The embedding process is achieved by using motion vectors of inter frames macroblocks, and, then discarding



Block size	*Bit-pair mapping*
16x16	00
16x8	01
8x16	10
8x8	11

Secret data	N				Y			
ASCII code	**01001110**				**01011001**			
Bit pairs	**01**	**00**	**11**	**10**	**01**	**01**	**10**	**01**
Mapped blocks	16x8	16x16	8x8	8x16	16x8	16x8	8x16	16x8

Fig. 7 Using mapping rules for prediction block type to conceal "NY" characters

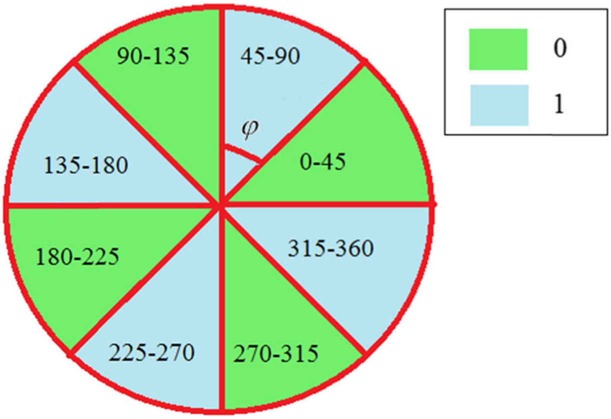


Fig. 8 Motion vector representation in [78]

the surrounding macroblocks. By using a predefined threshold, a group of motion vectors are selected in each video inter frame. The values (0 or 1) of selected motion vectors (MV_r) are obtained by calculating the phase angles (φ) illustrated in Fig. 8. By definition, phase angles are the arctangents of both vertical (MV_v) and horizontal (MV_h) motion vectors' components as given in Eq. 2.

$$\varphi = arctan\left(\frac{MV_v}{MV_h}\right) \left(0^{\mathring{A}} \leq \varphi_i < 360^{\mathring{A}}\right) \tag{2}$$

Once the MV_r values are obtained, the hidden information is concealed into the motion vector array utilizing the linear block code principle. The reason for using the linear block codes is to minimize the motion vectors' alteration rate and increase embedding capacity. The results of this algorithm have demonstrated that in every 6 bits of motion vector array, 4 bits of the secret data can be hidden. The pick signal to noise ratio (PSNR) of the obtained stego videos is 37.45 dB, which is proven by reducing alteration rate of motion vectors. However, this method has a limited hiding capacity due to it is based on the number of motion vectors. The data concealing and extracting phases of the Pan et al. method are illustrated in Eq. 3–6 as follows:

$$SY = MV_r H^T \tag{3}$$

$$b = SY \oplus S \tag{4}$$

$$MV_r^w = MV_r \oplus E_b \tag{5}$$

$$S' = MV_r H^T \oplus E_b H^T \tag{6}$$

Where S and $S^{'}$ are embedded and extracted messages. MV_r and MV_r^w are original and stego selected motion vectors. SY, E_b, and $H^T$are syndrome, coset leader of b, and transpose of parity check matrix, respectively [78]. Comparatively, Bin et al. [7] presented a new data concealing algorithm using the motion vector and matrix encoding processes. The naked eye can realize the difference that happens when the object moves tardily, while if the object transfers rapidly, then the change will be unnoticeable. The motion vectors that have large amplitudes are produced from the macroblocks that move quickly. The sizable motion vectors will be utilized for concealing the hidden message. The selected motion vectors for data embedding include two properties: 1) the motion vector's amplitude must be greater than the predefined threshold T; and 2) both the vertical and the horizontal motion vector components must not be equal. Moreover, the best component (MV_w) of both the vertical (MV_v) and the horizontal (MV_h) motion vectors are chosen based on their phase angles (θ). Then, the process of hiding the secret message is performed using matrix encoding, reducing the modification rate of selected motion vectors. The least significant bit (LSB) of the selected motion vectors (MV_{w_LSB}) is utilized for embedding secret bits. The average PSNR of the stego videos is 38.18 dB [7]. However, this algorithm has a low embedding capacity because the selected motion vectors have restricted conditions. The embedding stage of the algorithm introduced by Bin et al. can be carried out as follows:

$$MV_w = \begin{cases} MV_h & ;0 \le \theta < \pi/4 \\ MV_v & ;\pi/4 \le \theta < \pi/2 \end{cases} \tag{7}$$

$$\theta = \arctan|MV_v/MV_h| \tag{8}$$

$$MV_{w\_LSB} = \begin{cases} \text{unchanged} & ;\text{if } MV_w = 0 \\ 1 & ;\text{if } MV_{w\_LSB} = 0 \ and \ MV_w \ne 0 \\ 0 & ;\text{if } MV_{w\_LSB} = 1 \ and \ MV_w \ne 0 \end{cases} \tag{9}$$

In a different work, Jue et al. [35] designed a new algorithm for H.264/AVC video steganography using motion vectors as cover data. In this scheme, the luminance macroblocks for inter frames (P and B) video coding is used. Using a predefined threshold, the motion vectors with a large magnitude will be selected, while the motion vectors of slow objects will be discarded. Then, the hidden data bits will be concealed into the difference of both horizontal and vertical components for the selected motion vectors. This algorithm has improved the utilization ratio and the embedding efficiency. The modified motion vector's feature ($\hat{\mathrm{P}}_{\mathrm{i}}$) including the secret message can be calculated as follows:

$$\hat{P}_i = \begin{cases} mod\left[|V_{dx}| - |V_{dy}|, 2\right] & ;\text{if } P_i = S_i \\ mod\left[|V_{dx} + 0.25| - |V_{dy}|, 2\right] & ;\text{if } P_i \ne S_i \ and \\ & \quad |V_{dx}| - |V_{dy}| \ge 0 \\ mod\left[|V_{dx}| - |V_{dy} + 0.25|, 2\right] & ;\text{if } P_i \ne S_i \ and \\ & \quad |V_{dx}| - |V_{dy}| < 0 \end{cases} \tag{10}$$

P_i and S_i are motion vector features and secret message bits. V_{dx} and V_{dy} are horizontal and vertical motion vector components, respectively. However, Jue et al.'s scheme is limited to the embedding payload due to the high value of the predefined threshold. Commonly, the steganographic techniques that utilize the motion vectors as carrier objects to hide the secret messages, have low embedding capacities. Moreover, a high modification rate on the motion vectors will negatively influence the quality of the stego videos.

3.1.4 Video steganography techniques in transform coefficients (DCT, QDCT, and DWT)

The DCT, quantized discrete cosine transform (QDCT), and discrete wavelet transform (DWT) coefficients of the luminance component are also good candidates to conceal the secret message due to their low, middle, and high frequency coefficients for data embedding. Huang et al. [32] presented reliable information bit hiding using the DCT and communication theory. In order to enhance the robustness of this method, the BCH codes and soft-decision decoding have been used. Moreover, the robustness is also achieved by testing both the common signal processing operations and a StirMark attack. The secret data is hidden into the DCT coefficients, especially, in DC with the highest energy coefficient and low-frequency AC coefficients. Barni et al. [5] presented a watermarking technique of MPEG-4 video coding based on the video object planes. This scheme hides the watermark information into the selected inter and intra macroblocks of each video object. Depending on the computed frequency mask, the DCT coefficients that are greater than the predefined threshold are chosen for the embedding process. Barni's is flexible and easy to use for many applications. Moreover, it is robust against some common signal processing. Additionally, Shahid et al. [93] proposed a reconstruction loop for information embedding of intra and inter frames for H.264/AVC video codec. This method embeds the secret message into the LSB of QDCT coefficients. Only non-zero QDCT coefficients are chosen for data hiding process, utilizing the predefined threshold which directly depends on the size of secret information. Edges, texture, and motion regions of intra and inter frames are utilized in the concealing process. Shahid et al.'s algorithm extracts the hidden message easily and maintains the efficiency of compression domain. On the other hand, Thiesse et al. [100–102] presented a steganography of motion data in the chrominance and luminance of video frame components. In order to control the modification of the sum bitrate in the H.264 codec, the motion vector indices are embedded into the selected DCT coefficients of both luminance and chrominance components. In addition, the hidden indices minimize the distortion drift propagation of the prediction process to the next frames utilizing the rate-distortion optimization. The summation of the selected QDCT coefficients (S_i^w) is modified as follows:

$$S_i^w = \begin{cases} S_i \ ; \text{if } |S_i| \ mod2 = I_i \\ S_i + m_i \ ; \text{if } |S_i| \ mod2 \neq I_i \end{cases} \tag{11}$$

$$S_i = \sum_{n=1}^{N} a_n \tag{12}$$

Where a_n represents quantized coefficients, and S_i represents the summation of quantized coefficients of the i^{th} block. I_i is the prediction index and m_i represents shifted coefficients. Meuel et al. [64] proposed information concealing in H.264 codec for lossless reconstruction of the region of interest (ROI). This method protects the facial features of video stream by embedding facial regions into the DCT coefficients. Two LSBs of non-zero QDCT coefficients are utilized to embed the facial information. Only the skip mode is used during inter coded prediction of the ROI. Both DC and AC DCT coefficients of ROI macroblocks are set to 1 and 0, respectively, in order to guarantee predicting the original ROI macroblocks during the decoding process. The facial pixels are determined as skin pixels if the Euclidean distance is lower than the predefined threshold value d using the following formula:

$$\sqrt{(P_u - Ref_u)^2 + (P_v - Ref_v)^2} < d \tag{13}$$

Where P_u and Ref_u are the Cb and its reference components, respectively, P_v and Ref_v are the Cr and its reference components, respectively. The suggested method of Meuel et al. achieved a high quality of the region of interest based on the lossless reconstruction. In a different work, Yilamz et al. [109] proposed error concealment of video sequences by steganography. In the first stage, this method detects the location of the error which is the macroblocks that have been damaged. In the second stage, when the error location has been found, the distortion drift direction must be reversed, avoiding error propagation from other macroblocks. In the third stage, the reconstruction of the damaged macroblocks values is performed to fulfill successful error concealment. In Yilamz et al.'s algorithm, the edge information is hidden into the non-zero QDCT coefficients with the maintained bit-rate and channel utilization, and improved video quality. Later, Li et al. [44] proposed recoverable privacy protection for the video content distribution. This method utilizes DWT sub-bands of the region of interest in order to generate both a hidden message and a carrier. The middle and high frequency DWT coefficients are considered as carrier data, while the low frequency DWT sub-band is considered as secret information. The process of embedding is applied only on the luminance component. Additionally, Stanescu et al. [96] presented a video steganography algorithm called "StegoStream", which embeds the subtitle messages into the MPEG-2 video streams without using an extra bandwidth. In MPEG-2 compressed videos, the intra frames are self-dependent frames. Only the intra frames are used for the embedding process to hide video subtitles as secret messages. After the quantization process and the necessary predefined threshold T has been reached, the number of blocks are selected for data hiding. The LSBs of the non-zero DCT coefficients of the selected blocks that do not match with the hidden information bits alter; otherwise, the LSBs of the non-zero DCT coefficients remain unchanged. The video subtitle must appear in certain time. However, choosing an inconvenient threshold will cause the video subtitle to appear on the screen, incorrectly. Moreover, since the common MPEG-2 videos have 4–5 intra frames every one second, the video subtitles will not repeat continuously. Moreover, Li et al. [45] proposed a new algorithm for H.264 video steganography. During the video coding process, the quantized coefficients in each 4 × 4 luminance of inter frame macroblocks are used for embedding the secret message. The majority zero values of quantized coefficients are located on the bottom-right corner because it is a high frequency region. Conversely, the majority of non-zero values of quantized coefficients belonging to low frequency band are located on the top-left corner. An array of inverse zigzag scan mode equaled to every 16 quantized coefficients will be produced in order to obtain the last non-zeros more efficiently. Using a predefined threshold T (0–15), based on the scan point, the last non-zero coefficient is selected in every macroblock.

Depending on the parity of odd and even, the secret message of 1-bit per block is concealed. If the hidden bit is 1, then the selected DCT coefficients (V) modifies as follows:

$$\hat{V} = \begin{cases} V \ \ ;\text{if } V mod2 = 1 \\ V-1 \ \ ;\text{if } V mod2 = 0 | and \ V > 0 \\ V+1 \ \ ;\text{if } V mod2 = 0 \ | and \ V < 0 \end{cases} \tag{14}$$

Otherwise, the selected DCT coefficients (*V*) are modified as follows:

$$\hat{V} = \begin{cases} V \ \ ;\text{if } V mod2 = 0 \\ V+1 \ \ ;\text{if } V mod2 = 1 \ | and \ V > 0 \\ V-1 \ \ ;\text{if } V mod2 = 1 \ | and \ V < 0 \end{cases} \tag{15}$$

Li et al.'s method has limited data embedding payload because the selected blocks embed only one bit per 4 × 4 block. Correspondingly, both Ma et al. [60] and Liu et al. [54] presented a video data hiding for H.264 coding without having an error accumulation in intra video frames. In the intra frame coding, the current block predicts its data from the encoded adjacent blocks, specifically from the boundary pixels of upper and left blocks. Thus, any embedding process that occurs in these blocks will propagate the distortion, negatively, to the current block. In addition, the distortion drift will be increased toward the lower right intra frame blocks. To prevent this distortion drift, authors have developed three conditions to determine the directions of intra frame prediction modes. The 4 × 4 blocks have nine prediction modes (0–8) and 16 × 16 blocks have four prediction modes (vertical, horizontal, DC, and plane). In the 4 × 4 block, the first condition is the right mode $\{0, 3, 7\}$; the second condition is both the under-left mode $\{0, 1, 2, 4, 5, 6, 8\}$ and the under mode $\{1, 8\}$; and the third condition is the under right-mode $\{0, 1, 2, 3, 7, 8\}$. To select 4 × 4 QDCT coefficients of the luminance component for data embedding, the three conditions must be presented together. However, the two methods have a low embedding payload because only the luminance of the intra frame blocks that meet the three conditions are selected for hiding data. Later, Liu et al. [55, 56] presented a robust data hiding using H.264/AVC codec without a deformation accumulation in the intra frame based on BCH codes. By using the directions of the intra frame prediction, the deformation accumulation of the intra frame can be prevented. Some blocks will be chosen as carrier object for concealing the covert message. This procedure will rely on the prediction of the intra frame modes of adjacent blocks to prevent the deformation that proliferates from the neighboring blocks. The authors used BCH encoding to the hidden message before the embedding phase to enhance the method performance. Then, the encoded information is concealed into the 4 × 4 QDCT coefficients using only a luminance plane of the intra frame. Liu et al. defined *N* as a positive integer and $\widetilde{\mathrm{Y}}_{\mathrm{ij}}$ as selected DCT coefficients (i, j = 0,1,2,3). The embedding process of this method is carried out by the following steps:

1. If $\left|\widetilde{\mathrm{Y}}_{\mathrm{ij}}\right| = \mathrm{N}+1$ or $\left|\widetilde{\mathrm{Y}}_{\mathrm{ij}}\right| \neq \mathrm{N}$, then the $\widetilde{\mathrm{Y}}_{\mathrm{ij}}$ will be modified as follows:

$$\widetilde{Y}_{ij} = \begin{cases} \widetilde{Y}_{ij}+1 \ \ \text{if } \widetilde{Y}_{ij} \geq 0 \ and \ |\widetilde{Y}_{ij}| = N+1 \\ \widetilde{Y}_{ij}-1 \ \ \text{if } \widetilde{Y}_{ij} < 0 \ and \ |\widetilde{Y}_{ij}| = N+1 \\ \widetilde{Y}_{ij} \ \ \ \ \ \text{if } |\widetilde{Y}_{ij}| \neq N+1 \text{ or } |\widetilde{Y}_{ij}| \neq N \end{cases} \tag{16}$$

2. If the secret bit is 1 and $\left|\widetilde{Y}_{ij}\right| = N$, then the $\widetilde{Y}_{ij}$ will be changed as follows:

$$\tilde{Y}_{ij} = \begin{cases} \tilde{Y}_{ij} + 1 & \text{if } \tilde{Y}_{ij} \geq 0 \textit{ and } \tilde{Y}_{ij} = N \\ \tilde{Y}_{ij} - 1 & \text{if } \tilde{Y}_{ij} < 0 \textit{ and } \tilde{Y}_{ij} = N \end{cases} \tag{17}$$

3. If the secret bit is 0 and $\left|\widetilde{\mathrm{Y}}_{\mathrm{ij}}\right| = \mathrm{N}$, then the $\widetilde{\mathrm{Y}}_{\mathrm{ij}}$ will not be modified.

Overall, the previous methods that use DCT, QDCT, and DWT coefficients as venues to hide secret information are restricted to the limited number of coefficients in the embedding phase. Moreover, many mentioned algorithms did not include the secret message and cover data preprocessing stages which are necessary to improve security and robustness of any of the steganographic methods.

3.1.5 Video steganography techniques in entropy coding CAVLC and CABAC

During the H.264 compression, context adaptive variable length coding (CAVLC) and context adaptive binary arithmetic coding (CABAC) entropy coding can be used as host data to carry secret messages within many video steganography techniques. Ke et al. [38] presented a video steganography method relies on replacing the bits in H.264 stream. In this algorithm, CAVLC entropy coding has been applied in the data concealing process. During the video coding and after the quantization stage, authors used non-zero coefficients of high frequency regions for the luminance component of the embedding process. Here, non-zero coefficients in high frequency bands are almost "+1" or "-1". The embedding phase can be completed based on the trailing ones sign flag and the level of the codeword parity flag. The sign flag of the trailing ones changes if the embedding bit equals "0" and the parity of the codeword is even. Also, the sign flag changes if the embedding bit equals "1" and the parity of the codeword is odd. Otherwise, the sign flag of the trailing ones does not change. The trailing ones are modified as follows:

$$\textit{Trailing Ones} = \begin{cases} \textit{even codeword} & ; \textit{if secret bit} = 0 \\ \textit{odd codeword} & ; \textit{if secret bit} = 1 \end{cases} \tag{18}$$

The modification of high frequency coefficients does not have an impact on the video quality. However, the embedding capacity is low because Ke et al.'s method is established on the non-zero coefficients of the high frequencies that consist of a large majority of zeros. Similarly, Liao et al. [46] proposed real-time data concealing in H.264/AVC codec. During the process of CAVLC in 4 × 4 blocks, the trailing ones are utilized for embedding the secret data. The performance of this method was achieved through low computational complexity, negligible degradation of the video quality, and an unchangeable bit-steam size almost. This method employed random sequences as secret data. It is embedded into the selected blocks of CAVLC trailing ones as follows:

$$\hat{T}_{Ones} = \begin{cases} 2 & ; if\ w = 0\ and\ Trailing\ Ones \geq 3 \\ 1 & ; if\ w = 1\ and\ Trailing\ Ones = 2, \\ & or \\ & w = 1\ and\ Trailing\ Ones = 0 \\ \\ 0 & ; if\ w = 0\ and\ Trailing\ Ones = 1 \\ unchanged & ; otherwise \end{cases} \tag{19}$$

Where w represents secret data that is hidden into the trailing ones codeword within range of 0 to 3. $\hat{T}_{\mathrm{Ones}}$ represents modified trailing ones. Additionally, Lu et al. [58] proposed real-time frame dependent video watermarking in VLC coding. In order to achieve the real-time detection, the CAVLC encoder is applied during this algorithm. During the process of video coding, the secret data is embedded into the run-level pairs of each frame's macroblocks keeping the bit-rate almost unchangeable. Table 3 illustrates run-level pairs (r, l) and codewords of the CAVLC encoder. The diagram of the data hiding process was introduced by Lu et al., and is illustrated in Fig. 9.

Mobasseri et al. [65] proposed watermarking of MPEG-2 standard in a compressed domain by utilizing CAVLC mapping. During the CAVLC encoder, there are some run-level pairs that cannot systematically meet each other in intra frame blocks called unused pairs. The secret data is embedded into the codewords of unused run-level pairs of the CAVLC entropy coding. This method achieved a low modification rate of the selected run-level pairs which keeps the visual quality and bit-stream size of the watermarked video nearly unchanged. In a different work, Wang et al. [104] presented a real-time watermarking method in the H.264/AVC codec based on the CABAC features. The CABAC encoder uses a unary binarization, which is a process of concatenating all binary values of syntax elements. A certain number of motion vectors for both P and B frames are utilized for the data hiding process using the CABAC properties. The secret watermark is concealed by displacing the binary sequence of the selected syntax elements orderly. This method achieves a low degradation of the video quality because of the difference between the original code and the replacement code is very small (at most 1 bit is altered out 8-bits of the selected motion vector). This small

Table 3 VLC table (s denotes the sign bit)

(run, level)	Variable length code	Bit length
(0,1)	11 s	3
(0,2)	0100 s	5
(0,3)	0010 1 s	6
(0,4)	0000 110 s	8
(0,5)	0010 0110 s	9

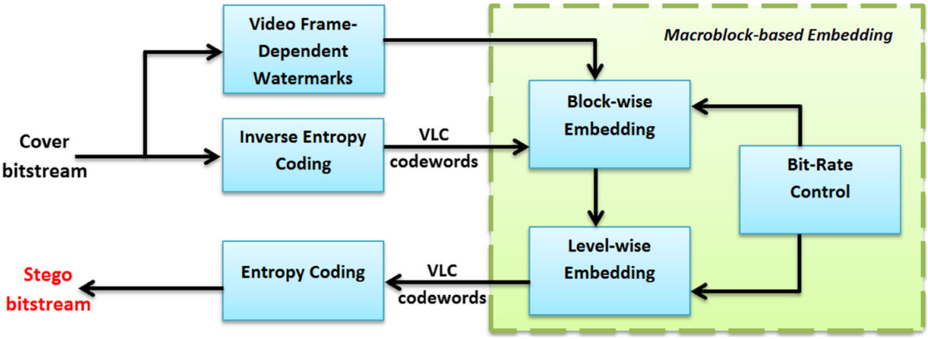


Fig. 9 Diagram of the hiding process in method [58]

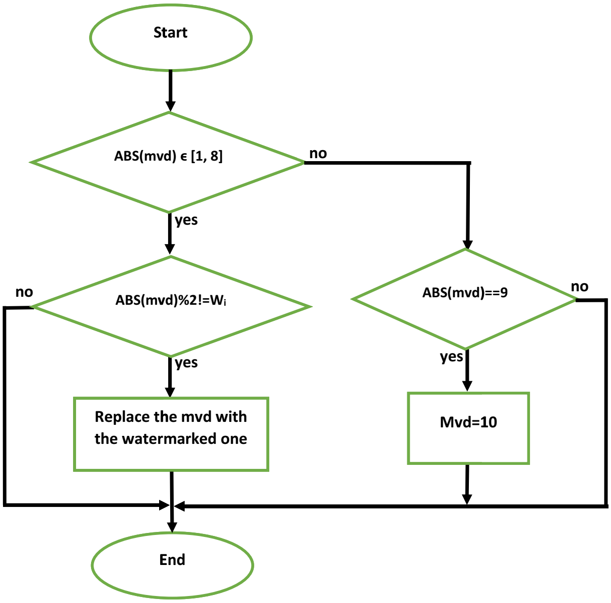
difference is also the reason of achieving a little bit-rate increase. The percentage of the increased bit-rate μ is calculated as follows:

$$\mu = \frac{m - u}{u} \times 100\% \tag{20}$$

where u and m indicate the bit-rate of the original and the watermarked videos respectively. The flowchart of this method is illustrated in Fig. 10. The diagram of the CABAC encoder is shown in Fig. 11. Generally, the previous methods that utilize CAVLC and CABAC entropy coding as venues to conceal secret messages are limited in capacity due to the restricted number of selected blocks in the embedding stage. Moreover, when using the entropy coding, the quality of the steganogram is severely distorted.

Table 4 summarizes video steganography methods that operate in compressed domain, emphasizing each of embedding capacity, video quality, robustness against attackers, video preprocessing, and secret messages preprocessing. Table 5 clarifies the advantages and limitations of each venue for

Fig. 10 The data embedding framework in [104]



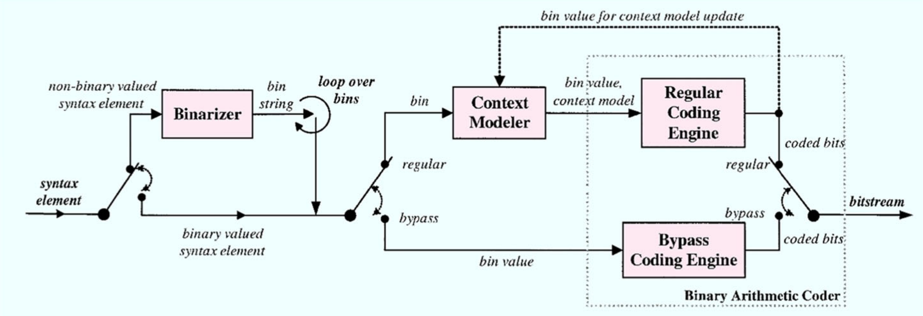


Fig. 11 General block diagram of the CABAC encoder

concealing secret messages in compressed domain. These venues include intra frame prediction, inter frame prediction, motion vectors, DCT coefficients, QDCT coefficients, DWT coefficients, CAVLC entropy coding, and CABAC entropy coding.

3.2 Video steganography techniques in raw domain

Unlike the compressed video, raw video steganography techniques deal with the video as a sequence of frames with the same format. First, digital video is converted into frames as still images, and then each frame is individually used as carrier data to conceal the hidden information. After the embedding process, all frames are merged together to produce the stego video. Raw video steganography techniques operate in both spatial and transform domains [75].

3.2.1 Video steganography techniques in spatial domain

There are many steganographic techniques that rely on the spatial domain such as LSB substitution, bit-plane complexity segmentation (BPCS), spread spectrum, ROI, histogram manipulation, matrix encoding, and mapping rule. Basically, these techniques utilize the pixel intensities to conceal the secret message. Zhang et al. [114] presented an efficient embedder utilizing BCH encoding for data hiding. This embedder hides the covert information into a block of carrier object. The concealing phase is achieved by modifying different coefficients in the input block to set the syndrome values null. This method enhances embedding payload and execution duration compared to others. The error correcting code (ECC) and steganographic model of this method is shown in the Fig. 12. Zhang et al.‘s method modifies the complexity of the algorithm from exponential to linear. On the other hand, Diop et al. [16] presented an adaptive steganography method utilizing the low-density parity-check codes. The method discusses how to reduce the influence of hidden information insertion by this codes. This algorithm demonstrated that the low-density parity-check codes are better for encoding algorithms than other codes. The process of embedding and extraction can be accomplished by Eq. 21 and Eq. 22.

$$S = \text{Embedding}\,(I, m) \tag{21}$$

$$m = \text{Extraction}\,(m) = HS \tag{22}$$

Table 4 Venues, embedding capacity, video quality, robustness, video and message preprocessing of the surveyed video steganography techniques that utilize compressed domain for data hiding

Technique	Domain / venue for data hiding	Embedding capacity	Video quality	Robustness	Video preprocessing	Message preprocessing
Liu et al. [53]	Compressed domain / Intra frame prediction	Low embedding capacity (only luma DCT coefficients of scene change Intra frames are used)	PSNR ranges 36 – 42 dB	Robust against video compression	Not used	Encryption
Chang et al. [9]	Compressed domain / Intra frame prediction	Average of embedding capacity ratio is 1.04 % (N bits per N × N DCT block of Intra frames)	37 dB when the bitrate is 20,000 Kb/s	Robust against HEVC compression	Not used	Not used
Hu et al. [31]	Compressed domain / Intra frame prediction modes	At most 1 bit per qualified Intra 4 × 4 luma block	Almost the same as compressed video	Robust against H.264/AVC compression	Not used	Not used
Zhu et al. [115]	Compressed domain / Intra frame prediction modes	At most 1 bit per qualified Intra 4 × 4 luma block	Almost the same as compressed video	Robust against H.264/AVC compression	Not used	Not used
Kapotas et al. [36]	Compressed domain / Inter frame prediction modes	Low embedding capacity (at most 3960 bits' capacity with the bitrate variation 85 % for 20 scene change frames of luma component of resolution 176 × 144)	Almost the same as compressed video	Robust against H.264 compression	Scene change detector	Not used
Xu et al. [107]	Compressed domain / Motion vectors	Low embedding capacity (at most 537 bits in 990 P-frame macroblocks, 4519 bits in 2640 B-frame macroblocks, and control information of each GOP in I-frame)	I-frame 35.22 dB, P-frame 34.61 dB, and B-frame 33.31 dB	Robust against MPEG compression	Not used	Not used
Pan et al. [78]	Compressed domain / Motion vectors	Low embedding capacity (at most 4 bits in 6 bits of high amplitude motion vectors and the modification of 2 bits)	Average PSNR is 37.45 dB	Robust against H.264 compression	Not used	Not used
Bin et al. [7]	Compressed domain / Motion vectors	Low embedding capacity (motion vector amplitude must exceed the	Average PSNR is 38.18 dB	Robust against H.264 compression	Not used	Not used

Table 4 (continued)

Technique	Domain / venue for data hiding	Embedding capacity	Video quality	Robustness	Video preprocessing	Message preprocessing
		threshold value and both components must not be equal)				
Jue et al. [35]	Compressed domain / Motion vectors	Low embedding capacity (at most 55 bits per P-frame or B-frames macroblocks. Largest amplitudes of motion vectors are used)	Average PSNR is 36.27 dB	Robust against H.264/AVC compression	Not used	Not used
Huang et al. [32]	Compressed domain / DCT coefficients	Low embedding capacity (32 character per frame/ image of resolution 352 × 288)	Average PSNR is 44 dB	Robust against StirMark 3.1 attack (signal processing)	Not used	BCH codes
Barni et al. [5]	Compressed domain / DCT coefficients	Low embedding capacity (at most 30 bits per video object of 500 Kb/s)	Almost the same as compressed video	Robust against MPEG-4 compression	Not used	Not used
Shahid et al. [93]	Compressed domain / QDCT coefficients	Average of embedding capacity ratio is 0.98 % (at most 195 kbps or 20 bits per macroblock)	Average PSNR is 43.39 dB	Robust against H.264/AVC codec	Not used	Not used
Thiesse et al. [100–102]	Compressed domain / QDCT coefficients	The motion vector indices are embedded into QDCT coefficients of luma and chroma	Almost the same as compressed video	Robust against H.264/AVC compression	Not used	Not used
Meuel et al. [64]	Compressed domain / QDCT coefficients	An average of 25 Kbits per frame when the bitrate is 3828 Kbits/s	Average PSNR is 47.71 dB when the bitrate is 3828 Kbits/s	Robust against H.264 compression	RIO (skin detection)	Not used
Yilamz et al. [109]	Compressed domain / QDCT coefficients	Intra frame: 8–13 bits of bit-length for resynchronization and 4 bits of edge-direction for damage. Inter frame: MV row hides in a corresponding row of the next frame	Y component: 36.00 dB, U component: 39.96 dB, V component: 41.24 dB when the bitrate is 500 Kbits/s	Robust against H.263+ codec	Not used	Not used
Li et al. [44]	Compressed domain / DWT coefficients	An average of 38 Kbits per frame of resolution	Average PSNR is 35.50 dB when the first level of DWT is used	Robust against JPEG/ JPEG2000 compression	RIO (object detection by GMM)	Not used

Table 4 (continued)

Technique	Domain / venue for data hiding	Embedding capacity	Video quality	Robustness	Video preprocessing	Message preprocessing
		352 × 288 when the first level of DWT is used				
Stanescu et al. [96]	Compressed domain / DCT coefficients	Low embedding capacity (an average of 1 bit per 8 × 8 block)	N/A	Robust against MPEG-2 codec	Not used	Not used
Li et al. [45]	Compressed domain / QDCT coefficients	Low embedding capacity (at most 1 bit per 4 × 4 luma block)	Average PSNR is 36 dB of Intra frame	Robust against H.264 codec	Not used	Not used
Ma et al. [60]	Compressed domain / QDCT coefficients	Average of embedding capacity ratio is 0.10 % (at average 798 bits per Intra frame of resolution 176 × 144) or (embedding ratio is 0.08 %)	Average PSNR is 40.74 dB of all Intra frames	Robust against H.264/AVC codec	Not used	Not used
Liu et al. [54]	Compressed domain / QDCT coefficients	Low embedding capacity (at average 758 bits per Intra frame of size 176 × 144 or 15,155 bits in 20 Intra frames)	Average PSNR is 40.73 dB of all Intra frames	Robust against H.264/AVC codec	Not used	Not used
Liu et al. [55, 56]	Compressed domain / QDCT coefficients	Average of embedding capacity ratio is 0.09 % (at most 3541 bits are embedded in 20 Intra frames of resolution 176 × 144)	Average PSNR is 46.35 dB of all Intra	Robust against H.264/AVC codec	Not used	BCH codes
Ke et al. [38]	Compressed domain / CAVLC	Embedding rate 2.44 % when quantization parameter (QP) =28 and video resolution is 352 × 288 or 1 bit per 4 × 4 residual block	Average PSNR is 34.54 dB when QP = 28 and video resolution is352 × 288	Robust against H.264 compression	Not used	Not used
Liao et al. [46]	Compressed domain / CAVLC	Low embedding capacity (at most 100 bits are embedded in 20th Intra frame of resolution 352 × 288)	Average PSNR is 34.37 dB when video resolution is 352 × 288	Robust against H.264/AVC codec	Not used	Not used

Table 4 (continued)

Technique	Domain / venue for data hiding	Embedding capacity	Video quality	Robustness	Video preprocessing	Message preprocessing
Lu et al. [58]	Compressed domain / CAVLC	N/A	Average PSNR is 37 dB	Robust against MPEG-2 codec and geometric attacks	Not used	Not used
Mobasseri et al. [65]	Compressed domain / CAVLC	Low embedding capacity (an average of 1 bit per 8 × 8 Intra block)	Almost the same as compressed video	Robust against MPEG-2 encoder	Not used	Not used
Wang et al. [104]	Compressed domain / CABAC	Average of embedding capacity ratio is 0.57 % (1156 bits are embedded in 50 frames of resolution 176 × 144)	Almost the same as compressed video (average PSNR is around 37.05 dB)	Robust against H.264/ AVC codec	Not used	Not used

Table 5 Advantages and disadvantages of each venue for data concealing in compressed domain

Venues for data hiding	Characteristics (According to compressed video steganography techniques)	Limitations
Intra frame prediction	The computational complexity is moderate	The embedding capacity is low and the impact on the video quality is high
Inter frame prediction	The influence on the video quality and the computational complexity are low	The embedding capacity is limited
Motion vectors	Both embedding payload and computational complexity are moderate	The impact on the video quality is high
DCT / QDCT / DWT coefficients	Achieve a high embedding payload as well as a low computational complexity	The influence on the video quality is high
CAVLC / CABAC entropy coding	Achieve a high embedding payload as well as a low computational complexity	The quality of the steganogram is severely distorted

Where I and S are the cover data and steganogram, respectively, and m is a secret message ($m \in F_2^m$). Additionally, Cheddad et al. [10] presented a skin tone data concealing method which depends on the *YCbCr* color space. *YCbCr* is utilized in different methods such as object detection and compression techniques. In *YCbCr*, the correlation between RGB colors is isolated by separating the luminance (*Y*) from the chrominance blue (*Cb)* and the chrominance red (*Cr*). Subsequently, the human skin areas are recognized, the *Cr* of these areas are used for concealing the hidden information. Overall, the method has a limited embedding capacity because the hidden message is embedded only in the *Cr* plane of the skin region. Similarly, Sadek et al. [91] proposed a robust video steganography method based on the skin region of interest. The secret message is concealed into the wavelet coefficients of skin regions for each blue and red components. This method is robust against MPEG compression. However, the results of comparison demonstrated that Cheddad et al.'s method outperformed Sadek et al.'s algorithm in both imperceptibility and embedding capacity. Khupse et al. [43] presented an adaptive information hiding scheme using steganoflage, which is based on the ROI in a frame instead of utilizing an entire frame. This method utilized human skin tone as a carrier object for concealing the hidden data. The filling operation and morphological dilation techniques have been applied as a skin detection. Then, the *YCbCr* frame that

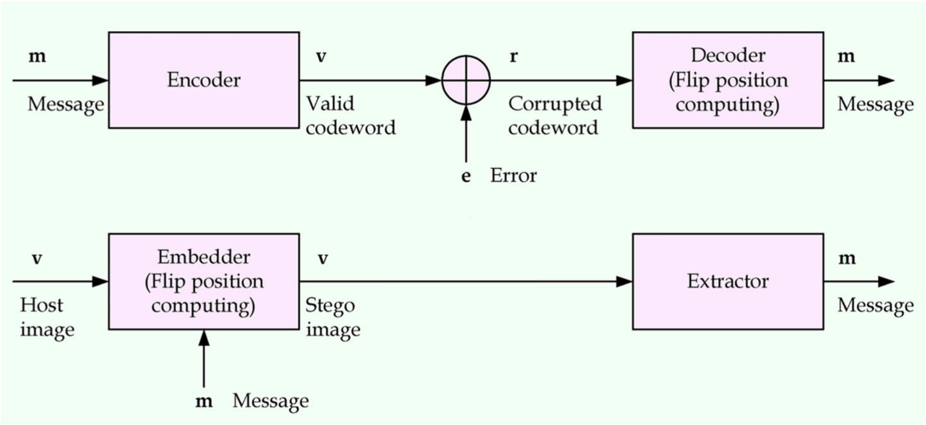


Fig. 12 ECC and steganographic method of [114]

has the lower mean square error (MSE) is chosen for the hiding stage. Only the *Cb* part of that certain video frame is selected for concealing the hidden information. Khupse et al.'s method is restricted in embedding payload due to considering only a single frame for data hiding stage.

Alavianmehr et al. [3] presented a robust uncompressed video steganography by utilizing the histogram distribution constrained (HDC). In this method, the *Y* component of every frame is segmented into non-overlapping blocks (*C*) of size $m \times n$. Then, the secret message is concealed into these blocks based on the shifting process. The selected blocks are changed only when the secret message bits are "1". The modified frame *S* of the k^{th} block is calculated as follows:

$$\hat{S}^k(i,j) = \begin{cases} S^k(i,j) + \gamma & ;\text{if } \alpha \in [0,T] \ and \ mod(i,2) = mod(j,2) \\ S^k(i,j) - \gamma & ;\text{if } \alpha \in [-T,0] \ and \ mod(i,2) \neq mod(j,2) \\ S^k(i,j) & ;\text{otherwise} \end{cases} \tag{23}$$

$$\gamma = \frac{(G+T) \times 2}{m \times n} \tag{24}$$

$$\alpha^k = \sum_{i=1}^{m} \sum_{j=1}^{n} C^k(i,j) \times N(i,j) \tag{25}$$

$$N(i,j) = \begin{cases} 1 & ;\text{if } mod(i,2) = mod(j,2) \\ -1 & ;\text{if } mod(i,2) \neq mod(j,2) \end{cases} \tag{26}$$

Where γ, α, and *N* are the shift quantity, the arithmetic difference, and the computed matrix for each block, respectively. Also, *T* and *G* are two predefined thresholds used in this method. Alavianmehr et al.'s method withstands against compression attack. However, it utilizes only *Y* plane for data embedding process. Similarly, Moon et al. [66] presented a secure data hiding method using a computer forensic process. The hidden message is authenticated and ciphered by a secret key, and then it conceals into the 4 LSB of each pixel of the video frames. In order to transfer the authentication key to the receiver, it will conceal into one of the frame recognized by the sender and recipient. The goal of utilizing the computer forensic process is the validity of the obtained stego videos. The method presented by Moon et al. is not robust against video processing operations due to utilization of spatial domain. In addition, Kelash et al. [39] presented a histogram variation-based video steganography method. Frames whose histogram variation averages exceed the histogram constant value (HCV) are chosen for the data concealing procedure utilizing the specified threshold. Then, these frames are segmented into blocks in order to compute the variation of the successive pixels. The hidden message is concealed into 3 LSB of each selected pixel. According to the hiding capacity, Kelash et al.'s method is restricted because it is only based on the HCV value. Comparatively, Paul et al. [80] presented a new steganographic technique to conceal the hidden message inside the video stream. Once the abrupt scene fluctuation frames are revealed, these frames are selected to host the hidden message. The histogram variation is utilized to find each frame whether it is a sudden scene variation or not. A 3–3-2 LSBs of each pixel are contributed into a data concealing process in order to hide the covert information. The randomization location of the pixels improved the security of this method. However, there is a limitation of the number of sudden scene changes frames. On the other hand, Bhole et al. [6] presented a randomization byte data hiding method. The first video frame is utilized to conceal the control data of other frames which is called an index frame. The remaining frames are used for data concealing procedure utilizing the index frame information. Bhole et al., also used the LSB method. Bhole et al.'s algorithm lacks of the robustness due to utilization of spatial domain. In a different work, Hanafy et al. [25] presented a secure communication method based on video steganography. This scheme is applied to the spatial domain by using raw videos as cover data and every text, audio, image, and video as a secret message. In this instance, the message is segmented into non-overlapping blocks, and then these blocks are randomly concealed into the frames based on the secret key. The randomization of the secret message is dynamically changed in each video frame in order to control identifying the message's location by attackers. The data embedding process is accomplished by using 2 LSBs of each color channel (RGB), which hides 6 bits of secret message in each pixel frame. In this scheme, the secret message is protected using a secret key. However, the scheme utilizes the spatial domain in order to embed the covert information. Here, this method is not robust against video compression processes and noises. Similarly, Lou et al. [57] proposed LSB steganography scheme using the reversible histogram transformation function. Here, the covert information is hidden into the LSB pixels of the cover data. This algorithm is robust against two well-known statistical steganalysis schemes including x^2-detection and regular-singular attacks. The average of the embedding rate of Lou et al.'s method is similar to the LSB technique. In addition, Tadiparthi et al. [99] proposed a steganographic method that utilizes animations as cover data. This method conceals the secret message into the animation frames. Tadiparthi et al.'s algorithm achieves better results when comparing with the two existing algorithms. However, the secret message distribution cannot be modified because the secret key relies on the probability distribution of the secret message. In addition, this method requires longer time to implement, and thus makes it more complex than others. Eltahir et al. [18] proposed a high rate data concealing algorithm. In each frame, a 3–3-2 approach is used based upon the LSB of three color channels (RGB). A 3–3-2 method refers to 3-bits of Red, 3-bits of Green, and 2-bits of Blue in each pixel that are used to hide the covert data as shown in the Fig. 13. Later, Dasgupta et al. [15] optimized the [18] method based on the genetic algorithm in order to enhance both the security of the covert information and the visual quality of the steganogram. The reason for this improvement is to develop an objective function that is based on the weights of different parameters such as MSE and HVS. However, [15, 18] algorithms are not robust against signal processing, noises, and video compression due to the fact that they operate in the pixel domain.

Hu et al. [30] presented a novel data concealing using a non-uniform rectangular partition method. The non-uniform rectangular partition procedure has three main factors. First, a suitable initial partition must be chosen to improve the results of the partition. Therefore, a reconstructed frame can be obtained with a minimum number of partitions and codes. Second, in order to make an approximation of the pixel gray values in each specific sub-image (rectangle), the bivariate polynomial has been utilized. Then, by applying the optimal quadratic approximation to these gray values, the undetermined coefficients of the bivariate polynomial can be specified. The partition processing will continue to divide the sub-image into four smaller parts, especially if the original sub-image cannot be extracted by the determined bivariate polynomial using the required control error. Also, the process of approximation is repeated again until the number of pixels in the sub-image is greater than or equal to the undetermined coefficients of the bivariate polynomial. The original image can approximately be reconstructed according to the codes that have been obtained from the partitioning process.

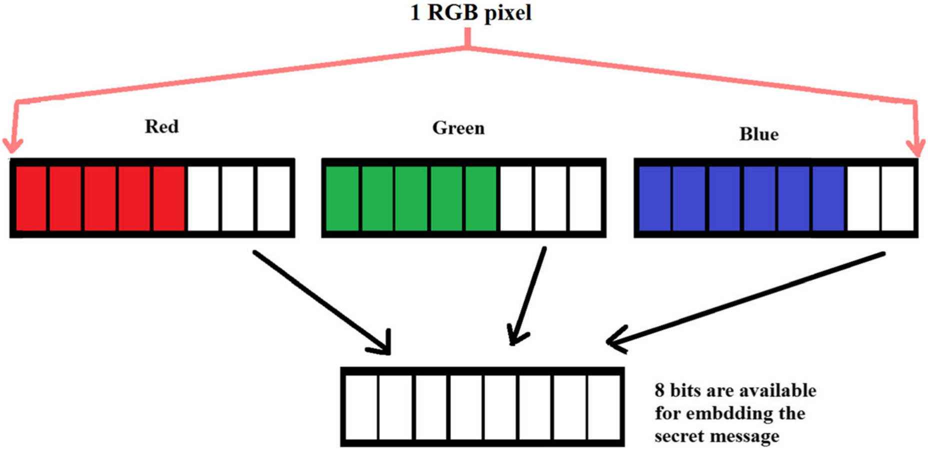


Fig. 13 The hiding capacity in each RGB pixel [18]

Third, the last factor of the non-uniform rectangular partition process is the control error. The control error is determined at the end of the partitioning process. It decides whether or not to continue dividing sub-images. The non-uniform rectangular partition is applied on each frame of secret video in order to obtain partitioned codes that will be concealed into the cover frames. This steganographic algorithm is based on a concept called "Tangram" that is similar to a puzzle game. The algorithm has two main advantages: 1) The adaptability of non-uniform rectangular partition and 2) the cover frame carries and records the partition codes information [30]. If the secret frame is A and the carrier frame is B, then the process of embedding in this method can be accomplished by the following points:

1- A suitable initial partition area is selected. Also, a control error $E = 4$ (ranged from 2 to 6) and a bivariate polynomial equation $f(x, y) = ax + by + cxy + d$ are specified. By applying the non-uniform rectangular partition algorithm, the frame A partition grids are obtained; and
2- Partition grids of frame A are placed on frame B, and then $h_1 = z_1 - \hat{z}_1$, $h_2 = z_2 - \hat{z}_2$, $h_3 = z_3 - \hat{z}_3$, and $h_4 = z_4 - \hat{z}_4$ are calculated. Where z_1, z_2, z_3, z_4 and $\hat{z}_1, \hat{z}_2, \hat{z}_3, \hat{z}_4$ are the gray values of each rectangular sub-area vertexes for A and B frames, respectively; and
3- Embedding all partition codes and their differences $\{h\}$ into each 4 LSB frame B gray values.

Hu et al.‘s algorithm increases the capacity of the hidden data. However, it is not robust against the video compression and temporal noises due to due to utilization of spatial domain. Moreover, the computational time is high due to algorithm's complexity. In a different work, Kawaguchi et al. [37] proposed principles and applications of BPCS steganography. In this method, the video frame is first converted into 8 bit-planes, and then each bit-plane is divided into informative (simple) and noise-like (complex) regions. The BPCS technique differs from the LSB technique in the number of bit-planes that are utilized for embedding secret message. The BPCS technique uses all bit-planes (0–7) for data hiding while the LSB technique only uses a bit-plane 0 for the embedding process. Figure 14 clarifies how one of the video frames converts to 8 bit-planes by applying the BPCS technique. In this method, the covert information is concealed into the complex regions to achieve a high embedding payload. Moreover, modifying the noise-like areas in each bit-plane for data hiding purposes has a minimal influence to the human visual system. The complexity (α) level is measured in each region whether informative or complex, and α can be defined as follows:

$$\alpha = \frac{k}{2m(m-1)}, (0\leq\alpha\leq1) \tag{27}$$

Where k equals the total length of the black-and-white border in the selected region, and $2m(m-1)$ is the highest possibility of the border length gained from the selected region. An $m \times m$ represents the size of the selected region. Figure 15 illustrates the complexity degree of the BPCS regions according to the Kawaguchi et al. method.

Sun [98] proposed a new information hiding method based on the improved BPCS steganography. The regular BPCS method computes the complexity of the selected region based on the total length of the black-and-white border. This technique introduces a new method that identifies the noise-like regions which is useful, especially, in periodical patterns. Each canonical gray coding (CGC), run-length irregularity, and border noisiness are utilized to measure the complexity level of the selected regions. Based on the complexity degree, the secret data is concealed into the noise-like areas. In order to expand the capacity of the covert information, the informative regions are converted into the complex regions using the conjugation operation. If n is the length of pixels and $h[i]$ is the repetition of run-lengths in each black-or-white of i pixels, then run-length irregularity of the binary pixels (H_s) in Sun's algorithm can be calculated as follows:

$$H_s = -\sum_{i=1}^{n} h[i]\ log_2 P_i \tag{28}$$

$$P_i = \frac{h[i]}{\sum_{j=1}^{n} h[j]} \tag{29}$$

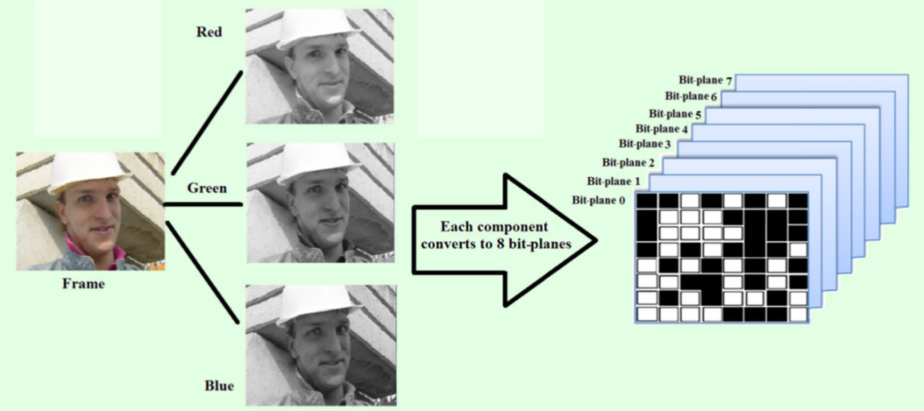


Fig. 14 The process of converting one of the Foreman video frames into 8 bit-planes using the BPCS technique

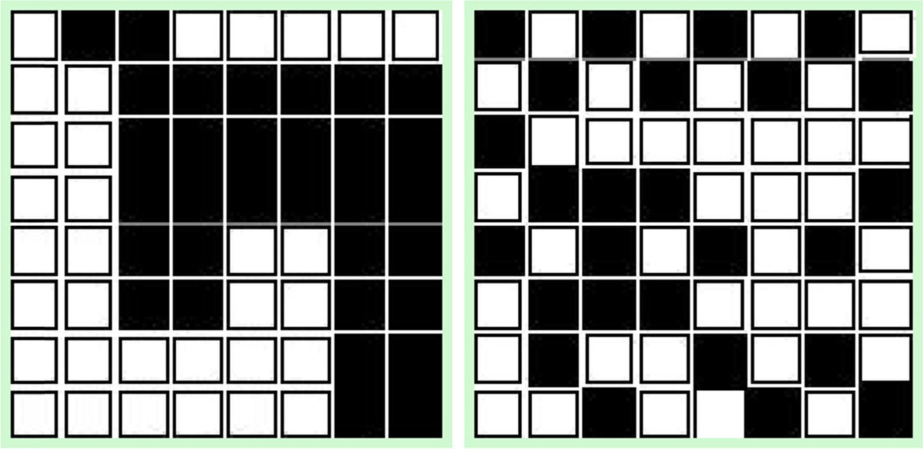


Fig. 15 BPCS complexity degree of different regions: left informative region and right noise-like region

In conclusion, the steganographic methods that operate in spatial domain are simple and obtain a high payload of secret messages. However, these techniques are not robust against signal processing, noises, and compression. Moreover, most of the above-mentioned methods do not take advantage of the cover data and the secret message preprocessing stages which can enhance the robustness and security of the steganographic algorithms.

3.2.2 Video steganography techniques in transform domain

In video steganography methods that operate in transform domain, each video frame is individually transformed into frequency domain using DCT, DWT, and discrete Fourier transform (DFT) and the secret message is embedded utilizing the low, middle, or high frequencies of the transformed coefficients. Patel et al. [79] presented a new data hiding method using the lazy wavelet transform (LWT) technique, where each video frame is divided into four sub-bands, separating the odd and even coefficients. The secret information is then embedded into the RGB LWT coefficients. For accurate extraction of embedded data, the length of hidden data is concealed into the audio coefficients. The amount of hidden information is high, but this type of wavelet is not a real mathematical wavelet operation. Consequently, Patel et al.'s method will not protect the hidden information from attackers due to it operates in the spatial domain. On the other hand, Spaulding et al. [95] presented the BPCS steganography method using an embedded zerotree wavelet (EZW) lossy compression. In this method, the DWT's coefficients are representing the original frame's pixels. Therefore, the BPCS steganography can be applied to DWT coefficient sub-bands which contain different features. The features of DWT sub-bands include correspondence, complexity, and resiliency against attacks. Each DWT sub-band is divided into pit-planes, and then the quantized coefficients are used for hiding the covert data. This method achieves a high embedding capacity around a quarter of the size of the compressed frame. Fig. 16 illustrates the data embedding process of Spaulding et al.'s method.

Similarly, Noda et al. [77] presented a video steganography technique utilizing the BPCS and wavelet compressed video. The 3D set partitioning in hierarchical trees (SPIHT) and motion-JPEG2000 are the two coding techniques that use the DWT domain. First, each bit-plane of the video frame and the secret message is segmented into 8*8 blocks. Then, the noise-like, bit-plane blocks are selected using the threshold of the noise-like complexity measurement. The two wavelet compression techniques are applied on the selected blocks by using the BPCS method, hiding the secret data into the quantized DWT coefficients. The experimental results of Noda et al.'s algorithm demonstrated that the 3D SPIHT coding method has a higher embedding payload than the Motion-JPEG2000 coding method when using BPCS steganography. However, the suggested algorithm of Noda et al. is not guaranteed that all types of cover videos contain enough noise-like bit-plane regions. Moreover, this method is only applied to the wavelet-based compression domain. Ordinarily, the steganographic techniques based on the transform domains improve the robustness against signal processing, noises, and compression. However, these techniques are more complex than the spatial domain methods.

Table 6 summarizes video steganography methods that utilize raw domain for data hiding, highlighting each of embedding capacity, video quality, robustness against attacks, video preprocessing, and secret messages preprocessing.

4 Performance assessment metrics

The main purpose of steganography techniques is to conceal the secret information inside the cover video data, thus the quality of the cover data will be changed ranging from a slight modification to a severe distortion. In order to evaluate whether the distortion level is acceptable or not, statistically, different metrics have been utilized

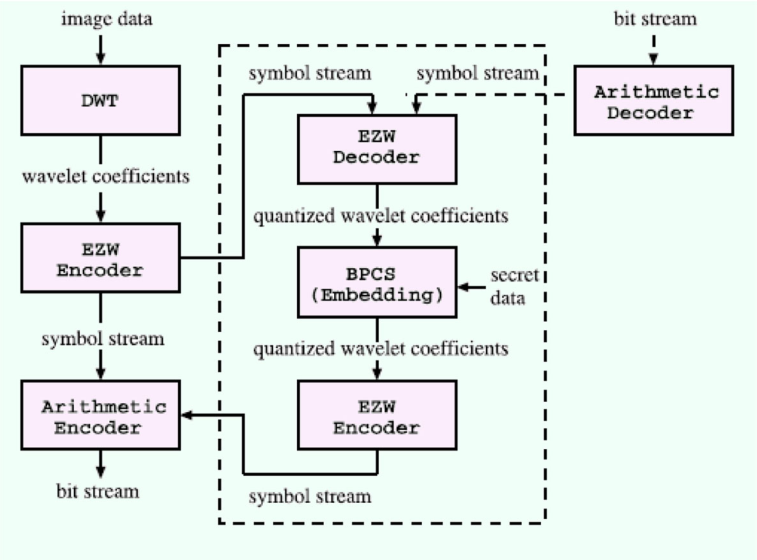


Fig. 16 A block diagram representing the data concealing phase of the method [95]

Table 6 Venues, embedding capacity, video quality, robustness, video and message preprocessing of the discussed video steganography methods that operate in raw domain

Technique	Domain / venue for data hiding	Embedding capacity	Video quality	Robustness	Video preprocessing	Message preprocessing
Zhang et al. [114]	Raw / Spatial domain	At most the embedding capacity is m × t bits per $n = 2^m - 1$ bits block, where $m > 2$ *and* $t = 2$ *or* 3	N/A	Not robust against signal processing operations	Not used	BCH
Cheddad et al. [10]	Raw / Spatial domain	Average of embedding capacity ratio is 0.08 %	Average PSNR is 61.22 dB	Not robust enough against signal processing and compression	Skin region detection	Not used
Cheddad et al. [12]	Raw / Spatial domain	Average of embedding capacity ratio is 1.03 %	Average PSNR is 59.63 dB	Not robust enough against signal processing and compression	Skin region detection	Not used
Sadek et al. [91]	Raw / Spatial domain	Average of embedding capacity ratio is 0.23 %	Average PSNR is 54.64 dB	Robust against MPEG-4 codec	Skin region detection	Not used
Khupse et al. [43]	Raw / Spatial domain	Low embedding capacity only frame is used (2120 bits per video)	Almost the same as original video	Not robust against signal processing, noises, and compression	Skin region detection	Not used
Alavianmehr et al. [3]	Raw / Spatial domain	Average of embedding capacity ratio is 1.34 % (4096 bits per video)	Average PSNR is 36.97 dB	Robust against H.264/AVC codec	Not used	Not used
Moon et al. [66]	Raw / Spatial domain	Average of embedding capacity ratio is 12.5 %	N/A	Not robust against signal processing, noises, and compression	Not used	Encryption
Kelash et al. [39]	Raw / Spatial domain	Average of embedding capacity ratio is 1.1 %	Average PSNR is 48.84 dB	Not robust against signal processing, noises, and compression	Not used	Not used
Paul et al. [80]	Raw / Spatial domain	Average of embedding capacity 8 bpp only in sudden scene change frames	Almost the same as original video (frames that are sudden scenes)	Not robust against signal processing and noises	Scene change detector	Not used
Bhole et al. [6]	Raw / Spatial domain	Average of embedding capacity ratio is 0.2 %	N/A	Not robust against signal processing, noises, and compression	Not used	Not used

Table 6 (continued)

Technique	Domain / venue for data hiding	Embedding capacity	Video quality	Robustness	Video preprocessing	Message preprocessing
Hanafy et al. [25]	Raw / Spatial domain	Average of embedding capacity 0.65 bpp	Average PSNR is 51.35 dB	Not robust against noises and compression	Randomization	Randomization
Lou et al. [57]	Raw / Spatial domain	Average of embedding capacity ratio is 12 %	Average PSNR is 50.51 dB	Robust against x^2-detection and regular-singular attacks	Not used	Not used
Tadiparthi et al. [99]	Raw / Spatial domain	Average of embedding capacity ratio is 2 %	N/A	Not robust against signal processing, noises, and compression	Not used	Encryption
Eltahir et al. [18]	Raw / Spatial domain	Average of embedding capacity 8 bpp	N/A	Not robust against signal processing, noises, and compression	Not used	Not used
Dasgupta et al. [15]	Raw / Spatial domain	Average of embedding capacity 8 bpp	Average PSNR is 38.45 dB	Not robust against signal processing, noises, and compression	Not used	Not used
Hu et al. [30]	Raw / Spatial domain	Average of embedding capacity 1.5 bpp	Average PSNR is 29.03 dB	Not robust against signal processing, noises, and compression	Not used	Non-uniform Rectangular Partition
Kawaguchi et al. [37]	Raw / Spatial domain	At most the embedding capacity ratio is 41 % when the threshold is 25	N/A	Not robust against signal processing and noises	BPCS	Not used
Sun [98]	Raw / Spatial domain	At most the embedding capacity ratio is 45 %	Average PSNR is 44.28 dB	Not robust against signal processing, noises, and compression	BPCS	Not used
Patel et al. [79]	Raw / Transform domain	Average of embedding capacity ratio is 12.5 %	Average PSNR is 31.23 dB	Not robust against signal processing, noises, and compression	Not used	Rijndael 256 encryption
Spaulding et al. [95]	Raw / Transform domain	Average of embedding capacity ratio is 25 %	Average PSNR is 33 dB	Robust lossy compression	BPCS	Not used
Noda et al. [77]	Raw / Transform domain	Average of embedding capacity ratios are 18 % for 1 bit-plane and 28 % for 2 bit-planes	Average PSNR of 2 bit-planes are 42.55 dB	Robust against 3D–SPIHT and Motion-JPEG2000 compression	BPCS	Not used

[2]. PSNR is a common metric utilized to calculate the difference between the carrier and stego data. The PSNR can be calculated as follows [92]:

$$MSE = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n}\sum_{k=1}^{h}[C(i,j,k)-S(i,j,k)]^2}{m \times n \times h} \tag{30}$$

$$\text{PSNR} = 10*Log_{10}\left(\frac{MAX_C{}^2}{MSE}\right)(dB) \tag{31}$$

C and *S* represent the carrier and stego frames. Both *m* and *n* indicate the frame resolutions, and *h* represents the RGB colors (k = 1, 2, and 3). *PSNR-HVS* (*PSNRH*) and *PSNR-HVS-M* (*PSNRM*) objective measurements are utilized to enhance the quality of the steganograms. The *PSNRM* is an upgraded form of the *PSNRH*. Each of *PSNRH* and *PSNRM* relies on the DCT coefficients of the transform domain [17]. *PSNRH* and *PSNRM* can be calculated using Eq. 32 and Eq. 33 [82]:

$$\text{PSNRH} = 10*Log_{10}\left(\frac{MAX_C{}^2}{MSE^{hvs}}\right)(dB) \tag{32}$$

$$PSNRM = 10*Log_{10}\left(\frac{MAX_C{}^2}{MSE^{hvs-m}}\right)(dB) \tag{33}$$

MSE^{hvs} and MSE^{hvs_m} utilize the factor matrix and the 8 × 8 DCT coefficients of the carrier and stego frame blocks [17]. On the other hand, the performance of steganographic method in terms of embedding capacity is a major factor that any method tried to increase it with the respect of the visual quality. According to [103], any steganographic method has a high hiding capacity if the hidden ratio exceeds 0.5 %. The embedding ratio is calculated in the following formula:

$$\text{Embedding ratio} = \frac{\text{Size of embedded message}}{\text{Cover video size}} \times 100\% \tag{34}$$

To further evaluate the performance of any steganographic algorithm in terms of robustness, two objective metrics including bit error rate (BER) and similarity are used. These metrics are applied to determine whether the secret messages are retrieved from the stego videos successfully by comparing the concealed and extracted covert data. The BER and similarity are computed in the following formulas [27]:

$$BER = \frac{\sum_{i=1}^{a}\sum_{j=1}^{b}\left[M(i,j)\oplus\hat{M}(i,j)\right]}{a \times b} \times 100\% \tag{35}$$

$$Similarity = \frac{\sum_{i=1}^{a}\sum_{j=1}^{b}\left[M(i,j) \times \hat{M}(i,j)\right]}{\sqrt{\sum_{i=1}^{a}\sum_{j=1}^{b}M(i,j)^2} \times \sqrt{\sum_{i=1}^{a}\sum_{j=1}^{b}\hat{M}(i,j)^2}} \tag{36}$$

Where M and $\hat{\text{M}}$ are the concealed and extracted hidden data, and, “*a*” and “*b*” are the size of the hidden data.

5 Conclusion and recommendations

In this paper, we have presented a comprehensive review and analysis of video steganography methods in both compressed and raw domains. In addition, the main confusion between steganography, cryptography, and watermarking techniques was eradicated. First, compressed video steganography techniques were classified based on the video encoding stages as venues for data embedding. Venues for concealing secret messages in compressed domain include: 1) intra frame prediction, 2) inter frame prediction, 3) motion vectors, 4) DCT and QDCT coefficients, and 5) CAVLC and CABAC entropy coding. Second, the existing raw video steganography methods were categorized according to their domain of operation including 1) spatial domain methods and 2) transform domain methods. Then, techniques of each domain were discussed and their performance assessments, imperceptibility, embedding capacity, robustness against attacks, video preprocessing, and secret messages preprocessing were highlighted. Furthermore, the characteristics and drawbacks of each steganographic method were mentioned. The following recommendations and future research trends are suggested to come up with an appropriate method for data hiding:

1- Proposing a video steganography method that maintains a trade-off between video quality, hiding capacity, and robustness against attacks, this makes it more appropriate for real-time security methods.

2- Suggesting a steganographic technique that combines steganography with other system protection methods such as cryptography and error correcting codes. Thus, encrypting and encoding the hidden massage prior to the embedding process will provide an additional security level to the secret message and make it more robust against attackers during the transmission.

3- Providing a video steganography algorithm that focuses on a portion of the video as carrier for data hiding instead of using entire video. Such a method will lead to enhance the quality of steganograms and the resistance against attacks. For instance, concealing the secret message into the region of interest includes human faces, human bodies, cars, or any other motion objects. Furthermore, it will be challenging for unauthorized users and intruders to define the position of hidden data in each video frames as the hidden data is concealed into the ROI which modifies from frame to frame, hence maintaining the security of hidden message.

4- Introducing a video steganography method that utilizes transformation coefficients of the ROI rather than using actual pixel domain. Since transform domain techniques are more robust against signal processing operations and compression process.

References

1. Abu-Marie W, Gutub A, Abu-Mansour H (2010) Image based steganography using truth table based and determinate Array on RGB indicator. Int J Signal and Image Process 1:196–204
2. Ahmad J, Sajjad M, Mehmood I, Rho S, Baik SW (2015) Saliency-weighted graphs for efficient visual content description and their applications in real-time image retrieval systems. J Real-Time Image Proc:1–17
3. Alavianmehr MA, Rezaei M, Helfroush MS, and Tashk A (2012) A lossless data hiding scheme on video raw data robust against H.264/AVC compression In: 2012 2nd International eConference on Computer and Knowledge Engineering (ICCKE), pp 194–198
4. Arsalan M, Malik SA, Khan A (2012) Intelligent reversible watermarking in integer wavelet domain for medical images. J Syst Softw 85:883–894

5. Barni M, Bartolini F, Checcacci N (2005) Watermarking of MPEG-4 video objects. IEEE Trans Multimedia 7:23–32
6. Bhole AT, Patel R (2012) Steganography over video file using Random Byte Hiding and LSB technique, In: 2012 IEEE. International Conference on Computational Intelligence & Computing Research (ICCIC), pp. 1–6
7. Bin H, Li-Yi Z, Wei-Dong Z (2011) A novel steganography algorithm based on motion vector and matrix encoding, In: 2011 IEEE. 3rd International Conference on Communication Software and Networks (ICCSN), pp 406–409
8. Chang F-C, Huang H-C, Hang H-M (2007) Layered access control schemes on watermarked scalable media. The J VLSI Sig Proc Syst Sig, Image, and Video Technol 49:443–455
9. Chang P-C, Chung K-L, Chen J-J, Lin C-H, Lin T-J (2014) A DCT/DST-based error propagation-free data hiding algorithm for HEVC intra-coded frames. J Vis Commun Image Represent 25:239–253
10. Cheddad A, Condell J, Curran K, McKevitt P (2008) Skin tone based Steganography in video files exploiting the YCbCr colour space, In: IEEE International Conference on Multimedia and Expo, 2008, pp 905–908
11. Cheddad A, Condell J, Curran K, Mc Kevitt P (2009a) A secure and improved self-embedding algorithm to combat digital document forgery. Signal Process 89:2324–2332
12. Cheddad A, Condell J, Curran K, Mc Kevitt P (2009b) A skin tone detection algorithm for an adaptive approach to steganography. Signal Process 89:2465–2478
13. Cheddad A, Condell J, Curran K, Mc Kevitt P (2010) Digital image steganography: survey and analysis of current methods. Signal Process 90:727–752
14. Das R and Tuithung T (2012) A novel steganography method for image based on Huffman Encoding, In: 2012 3rd National Conference on Emerging Trends and Applications in Computer Science (NCETACS), pp. 14–18
15. Dasgupta K, Mondal JK, Dutta P (2013) Optimized video steganography using genetic algorithm (GA). Procedia Technol 10:131–137
16. Diop I, Farss SM, Tall K, Fall PA, Diouf ML, Diop AK (2014) Adaptive steganography scheme based on LDPC codes. In: 2014 16th International Conference on Advanced Communication Technology (ICACT), pp. 162–166
17. Egiazarian K, Astola J, Ponomarenko N, Lukin V, Battisti F, and Carli M (2006) New full-reference quality metrics based on HVS In: CD-ROM proceedings of the second international workshop on video processing and quality metrics, Scottsdale, USA
18. Eltahir ME, Kiah LM, and Zaidan BB (2009) High rate video streaming steganography In: International Conference on Information Management and Engineering, ICIME ‘09. pp 550–553
19. Farschi S, Farschi H A novel chaotic approach for information hiding in image. Nonlinear Dyn 69:1525–1539 2012/09/01 2012
20. Fontaine C, Galand F (2007) How can reed-solomon codes improve steganographic schemes? In: Furon T, Cayre F, Doërr G, Bas P (eds) Information Hiding, vol 4567. Springer, Berlin, pp 130–144
21. Guangjie L, Weiwei L, Yuewei D, and Shiguo L (2011) An adaptive matrix embedding for image steganography, In: 2011 Third International Conference on Multimedia information networking and security (MINES) pp 642–646. doi:10.1109/MINES.2011.138
22. Guangjie L, Weiwei L, Yuewei D, Shiguo L (2012) Adaptive steganography based on syndrome-trellis codes and local complexity, In: 2012 Fourth International Conference on Multimedia Information Networking and Security (MINES), pp 323–327
23. Gutub AA-A (2010) Pixel indicator technique for RGB image steganography. J Emerging Technol Web Intell 2:56–64
24. Gutub A, Ankeer M, Abu-Ghalioun M, Shaheen A, Alvi A (2008) Pixel indicator high capacity technique for RGB image based steganography. In: WoSPA 2008-5th IEEE International Workshop on Signal Processing and its Applications, University of Sharjah, Sharjah, U.A.E. 18-20 March 2008
25. Hanafy A, Salama G, Mohasseb YZ (2008) A secure covert communication model based on video steganography, In: IEEE Military Communications Conference, 2008 MILCOM 2008 pp 1–6
26. Hasnaoui M, Mitrea M (2014) Multi-symbol QIM video watermarking. Signal Process Image Commun 29:107–127
27. He Y, Yang G, Zhu N (2012) A real-time dual watermarking algorithm of H.264/AVC video stream for video-on-demand service. AEU Int J Electron Commun 66:305–312
28. Horng S-J, Rosiyadi D, Li T, Takao T, Guo M, Khan MK (2013) A blind image copyright protection scheme for e-government. J Vis Commun Image Represent 24:1099–1105
29. Horng S-J, Rosiyadi D, Fan P, Wang X, Khan MK (2014) An adaptive watermarking scheme for e-government document images. Multimed Tools Appl 72:3085–3103
30. Hu S, KinTak U (2011) A novel video steganography based on non-uniform rectangular partition In: 2011 IEEE. 14th International Conference on Computational Science and Engineering (CSE), pp 57–61

31. Hu Y, Zhang C, Su Y (2007) Information hiding based on intra prediction modes for H. 264/AVC In: IEEE. International Conference on Multimedia and Expo 2007, pp 1231–1234
32. Huang J, Shi YQ (2002) Reliable information bit hiding. IEEE Trans Circuits Syst Video Technol 12:916–920
33. Huang H-C, Chu S-C, Pan J-S, Huang C-Y, Liao B-Y (2011) Tabu search based multi-watermarks embedding algorithm with multiple description coding. Inf Sci 181:3379–3396
34. Islam S, Modi MR, Gupta P (2014) Edge-based image steganography. EURASIP J Inf Secur 2014:1–14
35. Jue W, Min-Qing Z Juan-Li S (2011) Video steganography using motion vector components In: 2011 IEEE. 3rd International Conference on Communication Software and Networks (ICCSN), pp 500–503
36. Kapotas SK Skodras AN, (2008) A new data hiding scheme for scene change detection in H. 264 encoded video sequences, In: 2008 IEEE. International Conference on Multimedia and Expo
37. Kawaguchi E, Eason RO (1999) Principles and applications of BPCS steganography In: Photonics East (ISAM, VVDC, IEMB), pp 464–473
38. Ke N Weidong Z (2013) A video steganography scheme based on H. 264 bitstreams replaced In: 4th IEEE International Conference on Software Engineering and Service Science (ICSESS), pp 447–450
39. Kelash HM, Abdel Wahab OF, Elshakankiry OA, El-sayed HS (2013) Hiding data in video sequences using steganography algorithms, In: 2013 International Conference on ICT Convergence (ICTC), pp. 353–358
40. Khan A, Malik SA (2014) A high capacity reversible watermarking approach for authenticating images: exploiting down-sampling, histogram processing, and block selection. Inf Sci 256:162–183
41. Khan A, Malik SA, Ali A, Chamlawi R, Hussain M, Mahmood MT, Usman I (2012) Intelligent reversible watermarking and authentication: hiding depth map information for 3D cameras. Inf Sci 216:155–175
42. Khan A, Siddiqa A, Munib S, Malik SA (2014) A recent survey of reversible watermarking techniques. Inf Sci 279:251–272
43. Khupse S and Patil NN (2014) An adaptive steganography technique for videos using Steganoflage In: 2014 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), pp 811–815
44. Li G, Ito Y, Yu X, Nitta N, Babaguchi N (2009) Recoverable privacy protection for video content distribution. EURASIP J Inf Secur 2009:4
45. Li Y, Chen H-X Zhao Y (2010) A new method of data hiding based on H. 264 encoded video sequences, In: IEEE 10th International Conference on Signal Processing (ICSP), 2010 pp. 1833–1836
46. Liao K, Lian S, Guo Z, Wang J (2012) Efficient information hiding in H. 264/AVC video coding. Telecommun Syst 49:261–269
47. Lie W-N, Lin C-W (2006) Enhancing video error resilience by using data-embedding techniques, IEEE Trans Circuits Syst Video Technol 16:300–308
48. Lin W-H, Horng S-J, Kao T-W, Fan P, Lee C-L, Pan Y (2008) An efficient watermarking method based on significant difference of wavelet coefficient quantization. IEEE Trans Multimed 10:746–757
49. Lin W-H, Horng S-J, Kao T-W, Chen R-J, Chen Y-H, Lee C-L, Terano T (2009a) Image copyright protection with forward error correction. Expert Syst Appl 36:11888–11894
50. Lin W-H, Wang Y-R, Horng S-J, Kao T-W, Pan Y (2009b) A blind watermarking method using maximum wavelet coefficient quantization. Expert Syst Appl 36:11509–11516
51. Lin W-H, Wang Y-R, Horng S-J (2009c) A wavelet-tree-based watermarking method using distance vector of binary cluster. Expert Syst Appl 36:9869–9878
52. List P, Joch A, Lainema J, Bjontegaard G, Karczewicz M (2003) Adaptive deblocking filter. IEEE Trans Circuits Syst Video Technol 13:614–619
53. Liu B, Liu F, Yang C and Sun Y (2008) Secure steganography in compressed video bitstreams, In: Availability, Reliability and Security, ARES 08. Conference on Third International, 2008, pp 1382–1387
54. Liu Y, Li Z, Ma X, and Liu J (2012a) A novel data hiding scheme for H. 264/AVC video streams without intra-frame distortion drift In: IEEE 14th International Conference on Communication Technology (ICCT), 2012, pp 824–828
55. Liu Y, Li Z, Ma X and Liu J (2012b) A robust data hiding algorithm for H. 264/AVC video streams without intra-frame distortion drift, In: Proceedings of the 2012 Second International Conference on Electric Information and Control Engineering-Volume 01, pp 182–186
56. Liu Y, Li Z, Ma X Liu J (2013) A robust data hiding algorithm for H. 264/AVC video streams. J Syst Softw
57. Lou D-C, Hu C-H (2012) LSB steganographic method based on reversible histogram transformation function for resisting statistical steganalysis. Inf Sci 188:346–358
58. Lu C-S, Chen J-R, Fan K-C (2005) Real-time frame-dependent video watermarking in VLC domain. Signal Process Image Commun 20:624–642
59. Lusson F, Bailey K, Leeney M, Curran K (2013) A novel approach to digital watermarking, exploiting colour spaces. Signal Process 93:1268–1294
60. Ma X, Li Z, Tu H, Zhang B (2010) A data hiding algorithm for H. 264/AVC video streams without intra-frame distortion drift. IEEE Trans Circuits Syst Video Technol 20:1320–1330

61. Masoumi M, Amiri S (2013) A blind scene-based watermarking for video copyright protection. AEU Int J Electron Commun 67:528–535
62. Mehmood I, Sajjad M, Rho S, Baik SW (2016) Divide-and-conquer based summarization framework for extracting affective video content. Neurocomputing 174:393–403
63. Mercuri RT (2004) The many colors of multimedia security. Commun ACM 47:25–29
64. Meuel P, Chaumont M, Puech W (2007) Data hiding in H. 264 video for lossless reconstruction of region of interest, In: EUSIPCO 07: 15th European Signal Processing Conference, pp. 2301–2305
65. Mobasseri BG Marcinak MP (2005) Watermarking of MPEG-2 video in compressed domain using VLC mapping In: Proceedings of the 7th workshop on Multimedia and security, pp 91–94
66. Moon SK Raut RD (2013) Analysis of secured video steganography using computer forensics technique for enhance data security In: 2013 IEEE. Second International Conference on Image Information Processing (ICIIP), pp. 660–665
67. Mstafa R J Elleithy KM (2014) A highly secure video steganography using hamming code (7, 4) In: Systems, Applications and Technology Conference (LISAT), 2014 IEEE. Long Island, pp 1–6
68. Mstafa RJ Elleithy KM (2015a) A novel video steganography algorithm in the wavelet domain based on the KLT tracking algorithm and BCH codes In: IEEE Long Island Systems Applications and Technology Conference (LISAT), 2015, pp. 1–7
69. Mstafa RJ Elleithy KM (2015b) A high payload video steganography algorithm in DWT domain based on BCH codes (15, 11) In: Wirel Telecommunications Symp (WTS), 2015 pp 1–8
70. Mstafa RJ and Elleithy KM (2015c) A new video steganography algorithm based on the multiple object tracking and hamming codes In: 2015 IEEE 14th International Conference on Machine Learning and Applications (ICMLA), pp 335–340
71. Mstafa RJ, Elleithy KM (2016a) A DCT-based robust video steganographic method using BCH error correcting codes. IEEE Long Island Systems, Applications and Technology Conference (LISAT) 2016:1–6
72. Mstafa RJ, Elleithy KM (2016b) A video steganography algorithm based on Kanade-Lucas-Tomasi tracking algorithm and error correcting codes. Multimed Tools Appl 75:10311–10333
73. Muhammad K, Jamil A, Haleem F, Zahoor J, Muhammad S, Sung Wook B (2015a) A Secure Method for Color Image Steganography using Gray-Level Modification and Multi-level Encryption. KSII Transactions on Internet and Information Systems (TIIS) 9:1938–1962
74. Muhammad K, Mehmood I, Lee MY, Ji SM Baik SW (2015b) Ontology-based secure retrieval of semantically significant visual contents, arXiv preprint arXiv:1510.02177,
75. Muhammad K, Sajjad M, Mehmood I, Rho S, Baik S (2015c) A novel magic LSB substitution method (M-LSB-SM) using multi-level encryption and achromatic component of an image Multimed Tools Appl pp 1–27, 2015/05/24
76. Muhammad K, Sajjad M, Baik SW (2016) Dual-level security based Cyclic18 steganographic method and its application for secure transmission of Keyframes during wireless capsule endoscopy. J Med Syst 40:1–16
77. Noda H, Furuta T, Niimi M Kawaguchi E (2004) Application of BPCS steganography to wavelet compressed video, In: 2004 International Conference on Image Processing ICIP'04 pp 2147–2150
78. Pan F, Xiang L, Yang X-Y, Guo Y (2010) Video steganography using motion vector and linear block codes In: 2010 IEEE. International Conference on Software Engineering and Service Sciences (ICSESS), pp 592–595
79. Patel K, Rora KK, Singh K, and Verma S (2013) Lazy wavelet transform based steganography in video In: 2013 International Conference on Communication Systems and Network Technologies (CSNT), pp 497–500
80. Paul R, Acharya AK, Yadav VK Batham S (2013) Hiding large amount of data using a new approach of video steganography In: Confluence 2013: The Next Generation Information Technology Summit (4th International Conference), pp 337–343
81. Petitcolas FA, Anderson RJ, Kuhn MG (1999) Information hiding-a survey. Proc IEEE 87:1062–1078
82. Ponomarenko N, Silvestri F, Egiazarian K, Carli M, Astola J Lukin V (2007) On between-coefficient contrast masking of DCT basis functions. In: Proceedings of the Third International Workshop on Video Processing and Quality Metrics for Consumer Electronics, VPQM 2007, Scottsdale, Arizona, USA, 25-26 January 2007
83. Qazanfari K, Safabakhsh R (2014) A new steganography method which preserves histogram: generalization of LSB++. Inf Sci 277:90–101
84. Qian Z, Feng G, Zhang X, Wang S (2011) Image self-embedding with high-quality restoration capability. Digital Signal Process 21:278–286
85. Ritchey PC, Rego VJ (2012) A context sensitive tiling system for information hiding. J Inf Hiding and Multimed Sig Process 3:212–226
86. Robie DL, Mersereau RM (2002) Video error correction using steganography. EURASIP J Appl Sig Proc 2002:164–173
87. Rosiyadi D, Horng S-J, Fan P, Wang X, Khan MK, Pan Y (2012a) Copyright protection for e-government document images. IEEE MultiMedia 19:62–73

88. Rosiyadi D, Horng S-J, Suryana N, Masthurah N (2012b) A comparison between the hybrid using genetic algorithm and the pure hybrid watermarking scheme. Int J Comput Theory Eng (IJCTE) 4:329–331
89. Rupa C (2013) A digital image steganography using sierpinski gasket fractal and PLSB. J Inst Eng (India): Series B 94:147–151
90. Sadek MM, Khalifa AS, Mostafa MG (2015) Video steganography: a comprehensive review. Multimed Tools Appl 74(17):7063–7094
91. Sadek MM, Khalifa AS, Mostafa MG (2016) Robust video steganography algorithm using adaptive skin-tone detection. Multimed Tools Appl:1–21
92. Sajjad M, Muhammad K, Baik SW, Rho S, Jan Z, Yeo S-S, Mehmood I (2016) Mobile-cloud assisted framework for selective encryption of medical images with steganography for resource-constrained devices. Multimed Tools Appl:1–18
93. Shahid Z, Chaumont M, Puech W (2013) Considering the reconstruction loop for data hiding of intra-and inter-frames of H. 264/AVC. SIViP 7:75–93
94. Shanableh T (2012) Data hiding in MPEG video files using multivariate regression and flexible macroblock ordering. IEEE Trans Inf Forensics Secur 7:455–464
95. Spaulding J, Noda H, Shirazi MN, Kawaguchi E (2002) BPCS steganography using EZW lossy compressed images. Pattern Recogn Lett 23:1579–1587
96. Stanescu D, Stratulat M, Ciubotaru B, Chiciudean D, Cioarga R Micea M (2007) Embedding data in video stream using steganography In: 4th International Symposium on Applied Computational Intelligence and Informatics, 2007. SACI ‘07, pp 241–244
97. Subhedar MS, Mankar VH (2014) Current status and key issues in image steganography: a survey. Comput Sci Rev 13–14:95–113
98. Sun SL (2015) A new information hiding method based on improved BPCS steganography. Adv Multimedia 2015:1–7
99. Tadiparthi GR, Sueyoshi T (2008) A novel steganographic algorithm using animations as cover. Decis Support Syst 45:937–948
100. Thiesse JM, Jung J Antonini M (2010a) Data hiding of motion information in chroma and luma samples for video compression In: 2010 IEEE International Workshop on Multimedia Signal Processing (MMSP), pp 217–221
101. Thiesse JM, Jung J, Antonini M (2010b) Data hiding of intra prediction information in chroma samples for video compression In: 2010 17th IEEE International Conference on Image Processing (ICIP), pp 2861–2864
102. Thiesse JM, Jung J, Antonini M (2011) Rate distortion data hiding of motion vector competition information in Chroma and luma samples for video compression. IEEE Trans Circuits Syst Video Technol 21:729–741
103. Tse-Hua L, Tewfik AH (2006) A novel high-capacity data-embedding system. IEEE Trans Image Process 15:2431–2440
104. Wang R, HU L Xu D (2011) A watermarking algorithm based on the CABAC entropy coding for H.264/AVC. J Comput Inform Syst 7(6):2132–2141
105. Wang X-y, Wang C-p, Yang H-y, Niu P-p (2013) A robust blind color image watermarking in quaternion Fourier transform domain. J Syst Softw 86:255–277
106. Wedi T (2002) Adaptive interpolation filter for motion compensated prediction In: 2002 Proceedings International Conference on Image Processing II-509-II-512 2
107. Xu C, Ping X and Zhang T (2006) Steganography in compressed video stream In: International Conference on Innovative Computing, Information and Control, 2006. ICICIC’06. First pp 269–272
108. Yang G, Li J, He Y, Kang Z (2011) An information hiding algorithm based on intra-prediction modes and matrix coding for H. 264/AVC video stream. AEU Int J Electron Commun 65:331–337
109. Yilmaz A and Alatan AA (2003) Error concealment of video sequences by data hiding In: 2003 Proceedings International Conference on Image Processing, 2003. ICIP 2003. pp II-679-82 vol.3
110. Yiqi T, KokSheik W (2014) An overview of information hiding in H.264/AVC compressed video. IEEE Trans Circuits Syst Video Technol 24:305–319
111. Zhang X and Liu S (2012) Method and apparatus for intra mode coding in HEVC ed: Google patents
112. Zhang W, Cheung S-CS Chen M (2005) Hiding privacy information in video surveillance system In: ICIP (3), pp 868–871
113. Zhang R, Sachnev V, Kim H (2009) Fast BCH syndrome coding for steganography. In: Katzenbeisser S, Sadeghi A-R (eds) Information hiding, vol 5806. Springer, Berlin, pp 48–58
114. Zhang R, Sachnev V, Botnan MB, Kim HJ, Heo J (2012) An efficient embedder for BCH coding for steganography. IEEE Trans Inf Theory 58:7272–7279
115. Zhu H, Wang R, Xu D, and Zhou X (2010) Information Hiding Algorithm for H. 264 Based on the predition difference of Intra_4× 4 In: 2010 3rd International Congress on Image and Signal Processing (CISP), pp 487–490

Ramadhan J. Mstafa is originally from Duhok, Kurdistan Region, Iraq. He is pursuing his PhD degree in Computer Science and Engineering at the University of Bridgeport, Bridgeport, Connecticut, USA. He received his Bachelor's degree in Computer Science from the University of Salahaddin, Erbil, Iraq. Mr. Mstafa received his Master's degree in Computer Science from University of Duhok, Duhok, Iraq. He is an IEEE and ACM Student Member. His research areas of interest include image processing, mobile communication, security, watermarking, and steganography.

Dr. Khaled M. Elleithy is the Associate Vice President for Graduate Studies and Research at the University of Bridgeport. He is a professor of Computer Science and Engineering. He has research interests in the areas of wireless sensor networks, mobile communications, network security, quantum computing, and formal approaches for design and verification. He has published more than three hundred research papers in international journals and conferences in his areas of expertise. Dr. Elleithy has more than 25 years of teaching experience. His teaching evaluations are distinguished in all the universities he joined. He supervised hundreds of senior projects, MS theses and Ph.D. dissertations. He supervised several Ph.D. students. He developed and introduced many new undergraduate/graduate courses. He also developed new teaching / research laboratories in his area of expertise. Dr. Elleithy is the editor or co-editor for 12 books by Springer. He is a member of technical program committees of many international conferences as recognition of his research qualifications. He served as a guest editor for several international journals. He was the chairman for the International Conference on Industrial Electronics, Technology & Automation, IETA 2001, 19-21 December 2001, Cairo – Egypt. Also, he was the General Chair of the 2005-2014 International Joint Conferences on Computer, Information, and Systems Sciences, and Engineering virtual conferences.