Multimed Tools Appl
DOI 10.1007/s11042-014-1952-z

Video steganography: a comprehensive review

Mennatallah M. Sadek · Amal S. Khalifa ·
Mostafa G. M. Mostafa

Abstract Steganography is the art and science of secret communication, concealing the very existence of a communication. Modern cover types can take many forms such as text documents, audio tracks, digital images, and video streams. Extensive research has been done on image steganography in the previous decade due to their popularity on the internet. Nowadays, video files are drawing much more attention. They are transmitted more and more frequent on internet websites such as Facebook and YouTube imposing a larger practical significance on video steganography. Information hiding in video has a variety of techniques, each of which has its strengths and weaknesses. This paper intends to provide an up-to-date comprehensive review on the various video steganographic methods found in the literature in the last 5 years. Furthermore, since security and robustness are very important issues in designing a good steganographic algorithm, some relevant attacks and steganalysis techniques are also surveyed. The paper concludes with recommendations and good practices drawn from the reviewed techniques.

Keywords Video steganography · Information hiding · Spatial domain · Transform domain · Adaptive steganography

1 Introduction

The revolution in digital information has created new challenges for sending a message in a safe and secure way. Whatever method we choose, the most important question is its degree of security. Numerous approaches have been developed for addressing the issue of information security such as cryptography and steganography. Cryptography provides an obvious approach to securing information. It scrambles the secret message, such that it becomes meaningless to eavesdroppers. However, this is not always adequate in practice as the encrypted content itself

M. M. Sadek (✉) · A. S. Khalifa · M. G. M. Mostafa
Faculty of Computer and Information Sciences, Ain Shams University, Abassia, Cairo, Egypt
e-mail: menna.sadek@fcis.asu.edu.eg

A. S. Khalifa
e-mail: amal.khalifa@fcis.asu.edu.eg

M. G. M. Mostafa
e-mail: mgmostafa@cis.asu.edu.eg

Published online: 20 March 2014

draws attention. Regardless how strong is the encryption algorithm, given enough time and tools, it could be broken. Furthermore, some cases require sending information without anyone noticing that the communication happened. In such cases, steganography was the answer. Steganography is the art and science of invisible communication. The origin of the word steganography comes from the Greek language. It is derived from two Greek words "*stegos*" which means "cover" and "*grafia*" which means "writing" [18]. Steganography evolved driven by the need to hiding the existence of a secret communication.

Although cryptography and steganography try to protect data, but neither technology alone is perfect. Therefore, sometimes it is better to combine both approaches together to increase the security level of the system [53]. In this case, even if the communications existence was detected and the steganography was defeated, the attacker still has to break the encryption to know the message.

Watermarking is another technology that is closely related to steganography. But it lies on different philosophies and goals. Both technologies embed information in the cover in order to send this information imperceptibly. However, in steganography, the communication is carried out between two parties. As a result, steganography is mainly concerned with concealing the existence of the communication and protecting the embedded data against any modifications that may happen during transmission such as format change or compression. Thus steganography has limited robustness. On the other hand, watermarking techniques are used when the cover is available to parties who know the existence of the hidden information and may try to destroy it. An important watermarking application is the protection of intellectual properties of digital content [26, 27, 42, 70]. Hence the embedded information should be robust against intentional attacks that try to remove or change the watermark [34]. The literature contains various watermarking techniques such as [14, 29, 39, 43–45, 68, 71]

Table 1 shows a comparison between steganography, cryptography and watermarking. It highlights the similarities and differences between these three technologies.

The past decade has seen growing interests in steganography, especially in images and video. We found that most of the survey papers were dedicated to steganography in images and lacking a comprehensive review about the steganography in video. Al-Frajat et al. [5] only presents an overview of the subject. This leads to this review, in which we present a

Table 1 Comparison between steganography, cryptography and watermarking

	Steganography	Cryptography	Watermarking
Goal	Conceal the existence of the communications	Hide the contents of the communications	Protect the embedded content against intentional attacks for destruction or removal
Perceptual invisibility	Must Exist	Doesn't Exist	Application dependent
Signature size	Large	Large	Application dependent
Signature structure	May Change	Must Change	Doesn't Change
Use of key	Optional	Necessary	Optional
Output	Stego-file	Cipher text	Watermarked file
Goal fails when	Secret message existence is detected	Cipher text is decrypted	Watermark is changed or removed
Challenges	Perceptual transparency, Hiding capacity and robustness	Robustness	Robustness

comprehensive review of the literature in the last 10 years. In addition some applications of video steganography are discussed. And some images of covers are used to clarify the subject to the reader. Comparisons between the reviewed techniques in terms of advantages and disadvantages are provided. Also, we present a quick survey of steganalysis techniques to provide a comprehensive review on the subject. And finally, we present recommendations and good practices drawn from the reviewed techniques.

The rest of the paper is organized as follows: an overview of steganography is given in Section 2. Section 3 discusses the recent literature on video steganographic techniques. Performance measures are presented in Section 4. Section 5 describes the common steganalysis techniques. Finally, the paper is concluded in Section 6.

2 Steganography: an overview

Steganography means "covered writing". It is defined as the art of hiding information in ways that prevent the detection of hidden messages [32]. At the beginning, we briefly introduce the terminology used throughout the paper. The term "cover object" describes the file used for hiding information. The "secret message" refers to the data that is embedded in the cover through an embedding module. A "stego-object" is produced combining the cover object with the embedded data. In case of encrypting the secret message before embedding, an encryption key is used. This key is referred to as "stego-key". Furthermore, the term "steganalysis" refers to the different attacks that try to break the steganographic algorithm. Figure 1 shows a general steganographic model.

The design of a good steganographic technique faces many challenges. The algorithm's computational complexity and whether the algorithm is blind [28, 53, 93, 94] or non-blind should be considered. Unfortunately, most of the existing algorithms do not discuss their computational complexity. Mainly, there are four challenges: robustness, tamper resistance, hiding capacity and perceptual transparency. All of these aspects are inversely proportional to each other creating the data hiding dilemma. Robustness is the amount of modification the stego-object could withstand before an adversary destroys the hidden information [65]. While tamper resistance is the difficulty for an attacker to change the secret message after it has been embedded in the cover object. On the other hand, there is a trade-off between the hiding capacity and the perceptual transparency. When the hiding capacity increases, a smaller cover object could be used for hiding the secret message. This results a stego-object with a smaller size that can be easily transmitted over the internet. But increasing the hiding capacity leads to distortions in the stego-object. If an attacker recognizes the distortion, then the presence of the hidden message is detected. And at that point, steganography has failed as the secret communication was revealed.

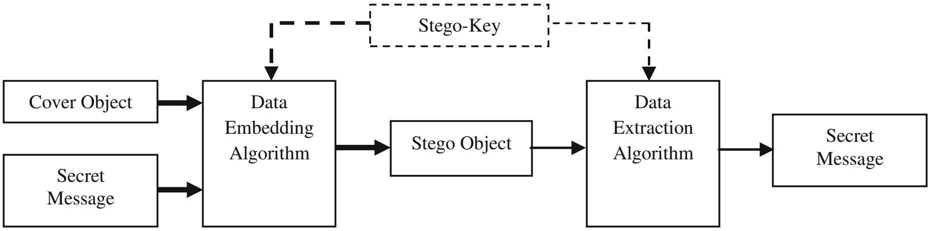


Fig. 1 General steganographic model. Embedding process is represented with bold arrows, while extraction process is represented with non-bold arrows

Thus, perceptual transparency is an extremely important feature of steganography. Stego-object noticeable distortions could uncover the secret communication. As a result some steganographic techniques follow a certain model that helps to decide the relevance of each of the pixels and the distortion level that the Human Visual System (HVS) cannot detect. These models are known as visual masking models. They make use of the physiological & psychological mechanisms of the HVS to do the masking effect. And they always use Just Noticeable Difference (JND) model. JND is defined as maximum distortion the human visual system cannot perceive. Wang et al. [97] implemented a visual masking model for images and videos that generates a relevance map of the image/frame in terms of 8x8 pixel blocks. Their model consists of three main components: JND Model, Visual Attention Model and Weighing Model. While Jia et al. [31] presented a JND model specifically designed for videos.

As for steganography cover types, almost any digital file format can be utilized for this purpose. But of course some formats are more appropriate than others for this job. Knowing that the primary goal of any steganographic technique is to maximize the hiding capacity and to minimize the embedding distortion, guide us to use file formats with higher redundancy. The redundant bits of an object are those bits that can be altered without the alteration being detected easily [6]. Based on the type of the cover object, steganography can be divided into six main types as illustrated in Figure 2.

Text steganography is a historic method of steganography. Modern techniques for text steganography include line-shift encoding [4, 47], word-shift encoding [37, 47] and feature specific encoding [62, 78]. Recently, text steganography is not used extensively. Text files have very limited amount of redundant data resulting in limited hiding capacity. In addition, text files could be altered easily leading to loss of the hidden message.

Another type of steganography is audio steganography. It can be viewed as hiding in a one dimensional signal. Audio steganography mainly depends on the masking phenomenon. This phenomenon indicates that a low audible sound turns to be inaudible if another louder audible sound existed [72]. Low-bit encoding, phase coding and spread spectrum, are examples of popular audio encoding techniques [50].

Images are the most popular cover objects used for steganography due to having a huge amount of redundant data. A digital image is a group of numbers that represent different light intensities in various areas of the image [32]. A grid is formed out from these numbers and each point on the grid is called a pixel. There are numerous digital image file formats. The most popular are Joint Photographic Experts Group (JPEG), Bitmap format (BMP) and Graphics Interchange Format (GIF). Different steganographic techniques exist for these file formats. For a detailed survey on steganography in images, interested readers can refer to [7, 17, 21, 75].

Video steganography, which is the focus of this review, can be viewed as an extension of image steganography. In fact, a video stream consists of a series of consecutive and equally time-spaced still images; sometimes accompanied with audio. Therefore, many image steganographic techniques are applicable to videos as well. Hu et al. [28], Shang [74], Langelaar et al. [38] and Sherly et al. [76], extended a number of image data hiding algorithms to video

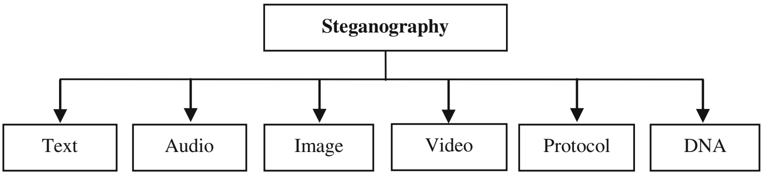


Fig. 2 Types of steganography according to the cover

proving this fact. Video is a very promising type of cover-media since it can carry a large amount of secret data. In addition, video steganography is becoming very important due to the frequent use and popularity of videos over the internet.

Protocol steganography is another type of steganography, which refers to embedding secret data within network packets. There are covert channels in the layers of the OSI network model where steganography can be used [23]. For example, Ahsan et al. [3] used some fields from the header of TCP/IP packet for hiding data. Mazurczyk et al. [51] presented the idea of retransmission steganography where a successfully received packet is intentionally not acknowledged to invoke retransmission. In this case, the re-transmitted packet carries the secret data instead of the original data.

Most recently, DNA-based steganography techniques actually gained a lot of attention. The high randomness in a DNA sequence can be utilized efficiently to hide any message without being noticed [67]. Therefore, DNA is a very good steganographic media, due to its tremendous storage capacity and the ability to synthesize DNA sequences in any desirable length.

3 Video steganographic techniques

Video streams have high degree of spatial and temporal redundancy in representation and have pervasive applications in daily life, thus they are considered as good candidates for hiding data. Video steganography can be then employed in various useful applications. One application is to use video steganography for military and intelligence agencies communications [59]. Another type of application was demonstrated by Robie et al. [69], Yilmaz et al. [96] and Lie et al. [41], where data hiding in video was used for video error correction during transmission or for transmitting additional data (e.g. subtitles) without requiring larger bandwidth [81]. A different application was presented by Zhang et al. [99], where video steganography was used for hiding data in a video captured by a surveillance system. That is, in order to protect the privacy of authorized people, their images are extracted from the surveillance video and embedded in its background.

Generally speaking, video steganography is the extension of image steganography. A video file can simply be viewed as a sequence of images, yielding video data hiding similar to image data hiding. However, there are many aspects that differentiate between video steganography and image steganography. As the video content is dynamic, lower chances of detection of the hidden data compared with images. In addition to the image attacks that can be applied on the separate frames of video; there are much more attacks for videos such as lossy compression, change of frame rate, formats interchanging, addition or deletion of frames during video processing. Handling a video stream as multiple two-dimensional images, does not consider the dependencies that exist among pixels in their three dimensions [2]. The hiding capacity is much higher in the case of video. Videos provide new dimensions for data hiding such as hiding messages in motion components. The audio components of the video file can also be utilized for data hiding.

Focusing on video steganographic techniques, we can classify them in a number of ways. One way is to categorize them according to compression, i.e. compressed video techniques [49, 58, 84] and uncompressed (raw) video techniques [93]; this classification was adopted by [76]. Another classification that can be used is based on the domain of embedding, i.e. spatial domain techniques [19, 22, 80] and transform domain techniques [11, 79, 95]. Moreover Shirali-Shahreza [77] suggested categorizing video steganographic techniques according to the following criteria: considering the video as a sequence of still images [19, 30]. Or finding new dimensions in the video that help in the steganographic process [49, 93]. Or utilizing the video saving format for information hiding [54]. Figure 3 shows these possible classifications.

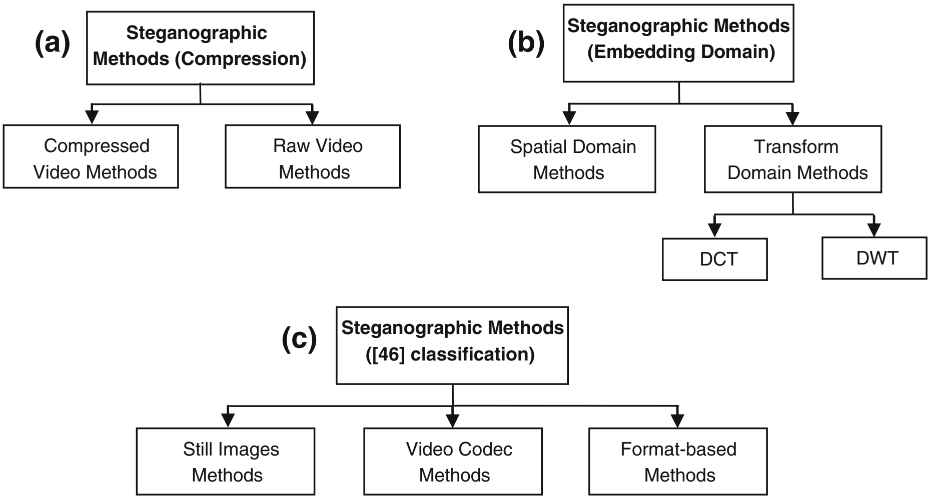


Fig. 3 **a**, **b**, **c** Various classifications of steganographic methods

But due to the diversity of the literature techniques, this survey adopted a detailed classification inspired from the existing ones. Although in some cases an exact classification may not be possible. Figure 4 illustrates the chosen classification.

The rest of this section is organized as follows: the reviewed techniques will be discussed in six subsections. Each subsection will briefly describe the general method and some related literature techniques.

3.1 Substitution-based techniques

Substitution-based techniques replace redundant data of the cover with the required secret message. Their main advantages are the implementation simplicity and the high embedding capacity relative to other techniques. Substitution-based techniques have numerous methods including the famous Least Significant Bit (LSB) technique, Bit Plane Complexity Segmentation (BPCS), Tri-way Pixel Value Differencing (TPVD), etc.

LSB is one of the oldest and most famous substitution-based techniques. In spite of its simplicity, it is capable of hiding large secret messages. It operates by replacing some LSBs of pixels from the cover video with the secret message bits. Our practical implementation of LSB is illustrated below. The secret message is a colored image of dimensions 670×670, and the cover is an AVI home video for a kid playing. The video has 14 frames each of dimensions 640×480. Figure 5 shows the first frame of cover video and the secret image. Table 2 presents the resulted stego-frames.

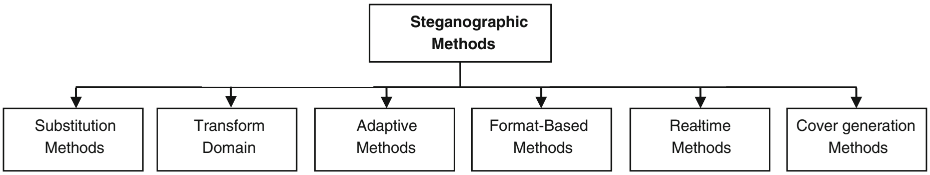


Fig. 4 Adopted classification for steganographic methods

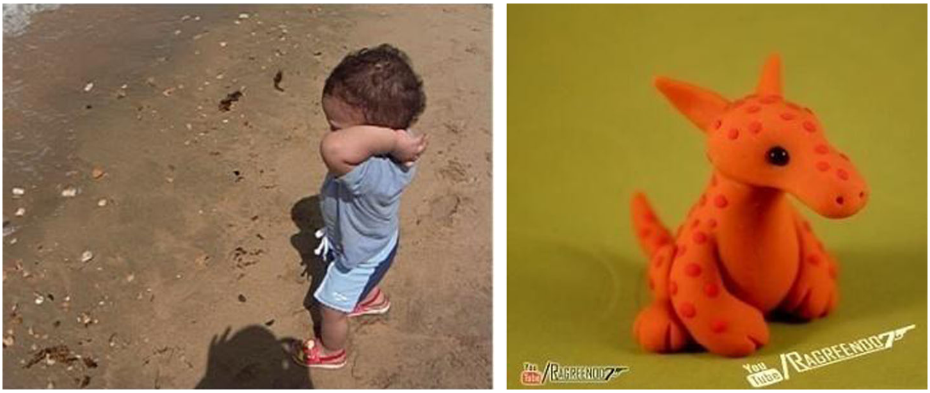


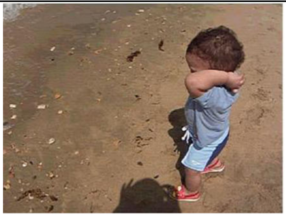
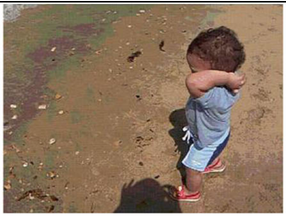
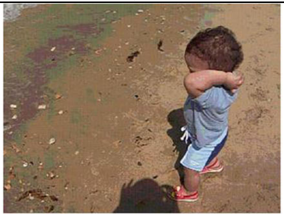
Fig. 5 **a** the first frame of the cover video before embedding. **b** the secret image to be hidden (http://ragreen007.blogspot.com/)

The above results show that the maximum number of least significant bits that could be used with acceptable visual distortion is 4 bits. Also, it is obvious that decreasing the number of color components used decreases the visual distortion as well.

Most of the substitution-based techniques that exist in the literature are actually inspired by the LSB method. For example, Singh et al. [80] used one least significant bit to hide a secret image in video. As a contribution for making analysis more difficult, the algorithm hides each row of the image pixels in the corresponding row(s) of multiple frames of the host video. That is, each row of pixels consisting of 8 bits is hidden in the first rows of multiple frames of the host. Hence, every 1 byte of image message needs 8 bytes from the host video frame(s). The algorithm is easy to implement. Furthermore, it uses only one least significant bit, so the visual distortion is minimal. But compared with other LSB techniques, the algorithm suffers from low capacity. Besides it is not highly secured.

Table 2 Illustrates the resulted stego-frames using 1 to 5 least significant bits for hiding

LSB= 1, RGB components
RMSE = 1.17, PSNR = 55.26
	
	LSB = 2, RGB components
	RMSE = 2.37, PSNR = 48.04
		
		LSB = 3, RGB components
		RMSE = 5.12, PSNR = 41.55


LSB = 4, RGB components
RMSE = 9.97, PSNR = 35.53
	
	LSB = 5, RGB components
	RMSE = 20.55, PSNR = 28.95
		
		LSB = 5, Red component only
		RMSE = 9.86, PSNR = 36.74

Many attempts were done for increasing the hiding capacity of LSB method and enhancing its perceptual transparency. As an example, Eltahir et al. [19] benefited from some HVS features to modify the traditional LSB method in a trial to achieve those enhancements. They utilized the fact that the human eye is more sensitive to the change in the blue level color compared to the red level and the green level colors. Their modification was to use 3-3-2 approach which means, using 3 least significant bits from red color and 3 from green color but only 2 from blue color. This algorithm uses 33.3 % of each video frame for data hiding. But still the algorithm is neither tamper resistant nor robust.

More LSB-based techniques were proposed in an attempt to enhance its tamper resistance. For example, Hu et al. [28] presented an algorithm for hiding video in video using LSB. Their algorithm applies an important pre-processing step. Each frame of the secret video undergoes a process called non-uniform rectangular partitioning [85]. Non uniform rectangular partitioning is an image coding technique. Each video frame is divided into rectangles with varying dimensions. Then optimal quadratic approximation is used for approximating the values in each sub-rectangle. A bivariate polynomial is used for the optimal quadratic approximation. The output of this process is the partition codes and partitioning grids. Figure 6 shows an example of lena partitioned image using this technique.

The encoding process starts by calculating the partition grids of the secret frame by using non-uniform rectangular partitioning. Then place the calculated partition grids onto the cover frame and calculate the difference between the values of the four vertices of each rectangular sub-area as follows:

- Read the values of the four vertices of each sub-rectangle for both images over the grid {z} and {z′}
- Calculate the differences $h_1=z_1 - z_1'$, $h_2=z_2 - z_2'$, $h_3=z_3 - z_3'$ and $h_4=z_4 - z_4'$

Finally all of the partition codes and the calculated differences are hidden in the cover frame using the four least significant bits. The application of the non-uniform rectangular partitioning algorithm shrinks the size of the secret video and also, adds security to the hiding algorithm as the partition codes can be considered an encrypted version of the original video. This technique showed a high hiding capacity while the authors considered the high encoding and decoding speed of the non-uniform rectangular partition algorithm as an advantage. However, the main disadvantage of this technique is the inaccurate retrieval of the secret bits due to changes in the original pixel values causing a problem in the decoding phase (inverse of difference) which leads to poor PSNR of the extracted frames.

Another modification to the LSB method was presented by Hanafy et al. [22]. They partitioned the secret message into non overlapping blocks before hiding. Then each video

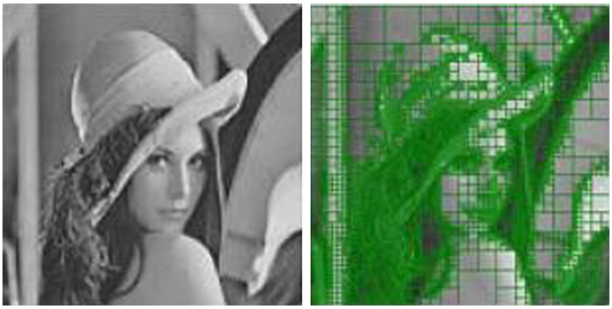


Fig. 6 **a** Original Image **b** resultant grid from partitioning overlaid on the original image [85]

frame is assigned a number of blocks for embedding. A stego-key is used for calculating the locations of the blocks, from its re-orderings. The re-ordering is changed dynamically with each frame to overcome the possibility of statistically identifying the secret message locations. Finally, the stego-key data is embedded in a specific row in the cover video frame calculated using an agreed upon formula. The embedding process consumes two least significant bits from each color component in each pixel. However, the experimental results showed that despite of the pre-processing done on the secret message, the method is not tamper resistant or robust to compression.

On another side, the simple implementation and the low computational complexity of LSB method drew the attention for implementing the idea of real time steganography. Shirali-Shahreza [77] used the LSB method for hiding a secret message in the frames displayed by the output screens of instruments, such as electronic advertising billboards. He considered each frame displayed as an image, which is then broken down into small blocks where the secret message is hidden. For photographing the frames displayed and extracting the secret message, the secret data is hidden redundantly in a large number of frames. A modification to this method was then proposed by Channalli et al. [15], where a secret key was used for securing the embedding process. The first and second bytes of the key are used to divide the frame displayed into a number of smaller blocks. The rest of the key - which they call pattern bits - is used along with the secret message bits to change the LSBs of the pixels. A single bit of the secret message is embedded in the whole block to allow for precise extraction. Both methods can be applied for broadcasting a secret message in a public place such as railway stations, airports and stadiums. It does not need any storage space giving the capability of hiding large secret messages in real-time. Also, there is no cover media available for doing any analysis. On the other hand, to implement this method, a special device needs to be attached to the electronic billboard to perform the hiding process in real-time. Furthermore, the photographing process itself is sensitive to the environmental effects and hence, it requires the use of an advanced camera. Also, if the receiver misses photographing a certain frame, then part of the secret message will be lost.

Generally speaking, the idea behind the LSB method is to replace the least significant bits of pixels with the secret data, which leads to deteriorating the quality as more significant bits are used. This led to the evolution of other methods, trying to overcome this disadvantage, such as the Bit Plane Complexity Segmentation BPCS [35] and Tri-Way Pixel-Value Differencing [13]. BPCS benefits from the fact that the HVS cannot receive figure information in a complicated binary pattern. BPCS could be applied either in the spatial domain [30] or in the transform domain [58]. The idea of BPCS is to decompose an image/frame into bit planes. A bit plane can be considered as a slice of the image that is made up from all the bits of a specific significant position from each binary digit. After decomposing the image into bit planes, the complexity of each region in the bit planes is measured. Regions are categorized to either informative or noise-like. The noise-like regions are then replaced with the secret data with minimum effect on the perceived quality. Figure 7 illustrates an example of a noise-like region and an informative one.

Jalab et al. [30] adopted the BPCS for hiding data in selected MPEG video frames. Their technique works in the YCbCr colorspace for removing the correlation between the red, green and blue components of a pixel and decreasing the distortion caused by embedding. It is well known that the human eyes are sensitive to changes in smooth areas rather than noise-like ones. Thus, the BPCS methodology was utilized for measuring the complexity of each region in the cover frame. The complexity of each part of the bit plane is calculated as the number of non edge transitions from 1 to 0 and 0 to 1, both horizontally and vertically. Their technique also allows the selection of the starting and ending frames for the hiding process.

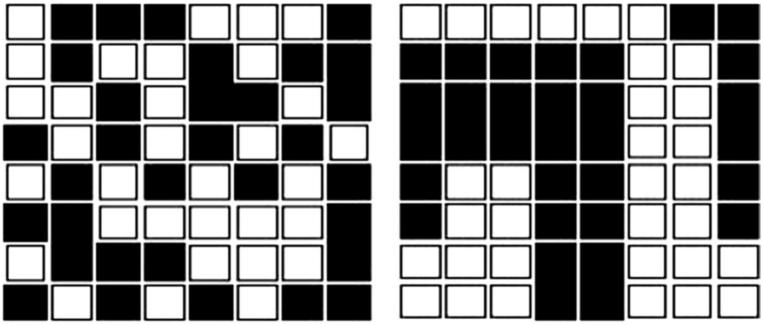


Fig. 7 **a** Noise-like region **b**. Informative region [30]

Another substitution-based technique is the Tri-way Pixel-Value Differencing (TPVD) [13]. In fact, it is a modified version of the popular Pixel-Value Differencing (PVD) method. PVD hides the secret data in the difference value of two adjacent pixels. Difference values are classified into ranges, where each range has lower bound, upper bound and width. Smaller range index indicates a smooth area where less data can be hidden, while larger range index indicates a sharp area where more data can be hidden. The hiding process starts with partitioning the cover image/frame into non-overlapping blocks of two adjacent pixels. Second, the difference value and its range are determined. Third, the number of secret bits to be hidden is calculated based on the range index. Finally, the required number of secret bits is extracted from the secret message and their corresponding decimal value is used to produce a new difference and the pixel values are adjusted accordingly. The TPVD method; on the other hand, embeds data in all horizontal, vertical and diagonal edges providing more hiding capacity. TPVD was used by Sherly et al. [76] to embed data in MPEG compressed videos. According to their approach, secret data are embedded in the macro-blocks of the "I" frame with maximum scene change and in macro-blocks of the P and B frames with maximum magnitude of motion vectors. The authors presented two adaptive rules named branch conditions, to control the amount of change caused by TPVD, so as to keep the distortion to the minimum.

3.2 Transform domain techniques

Although substitution-based techniques are considered the simplest way for information hiding, but their main disadvantage is the vulnerability to any cover modification including compression, format change, etc. In addition, the embedded data using these techniques can be easily destroyed by an attacker. Transform domain techniques are more complex, but in return, they try to enhance the robustness and the perceptual transparency of the produced stego-objects. Basically, any transform-domain technique consists of at least the following steps: First the cover is transformed into the frequency domain, then secret message is embedded in some or all of the transformed coefficients, and finally the modified coefficients are transformed back to the original form of the cover. Examples of these transforms include: Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT). Discrete Fourier Transform (DFT) methods are not so popular in steganography. According to Raja et al. [63], DFT methods introduce round-off errors that do not make them ideal for information hiding applications. However, few techniques in the literature used DFT based steganography such as McKeon [52] who used the 2D DFT for steganography in movies.

Discrete Cosine Transform (DCT) is a very popular transform. It is broadly used in image and video compression methods. It may be applied in block-wise or frame-wise manner. One of the early algorithms in this field was presented by Chae et al. [11] using texture masking and multidimensional lattice structure. They used MPEG-2 compressed videos. Both the secret message and the cover video frames are transformed using 8x8 block DCT. The secret message coefficients are quantized then encoded using the multidimensional lattices, and finally embedded into the cover frame DCT coefficients. The embedding is adaptive to the local texture content of the cover video frame blocks. 16 host video DCT blocks are required to embed one signature 8x8 DCT block. Furthermore, the extraction process can be made blindly. Figure 8 explains the hiding process.

Increasing the hiding capacity without affecting visual quality is one challenge facing steganographic techniques. High bitrate techniques aim at hiding relatively large amount of secret information in the cover. Yang et al. [95] designed a high bitrate algorithm that works on H.264/AVC Compressed videos. First, the cover video frames are converted to the YUV color space. Then, 1 bit is hidden in each 4×4 DCT coefficient block with means of vector quantization. Beside the ability to hide large amount of data, their algorithm is robust to H.264 and MPEG-4 compression techniques and it is tamper resistant. The only limitation is the trade-off between robustness to compression and visual distortion. Figure 9 illustrates the detailed steps of the hiding algorithm. The high hiding capacity of the algorithm was used by Shou-Dao et al. [79] for hiding video in video while keeping the file size of the host video fixed after the hiding process.

Sequential video frames look similar to each other except the frames at scene change or the frames with high motion. This makes it possible to add or drop or even re-order some successive frames without causing noticeable degradation. Since common video processing can cause frame adding, dropping or deletion, these operations must be taken into account when embedding secret data. Xu et al. [94] solved this problem by redundant data embedding. They utilized I, P and B frames of MPEG videos. Control information needed for data extraction is embedded in I frames. While, the secret message itself is repeatedly embedded in motion vectors of high motion in P and B frames. The embedding in motion vectors was derived from the algorithm of Jun Zhang et al. [100]. The proposed embedding process causes little distortion because of selecting motion vectors with large magnitudes. Furthermore, the algorithm is robust to video processing (frame adding, frame dropping or re-ordering of adjacent frames) and the extraction is blind. The only problem is that the hiding capacity is affected by the redundant embedding of the secret message and the control information. This makes the algorithm ideal for watermarking rather steganography.

Discrete Wavelet Transform (DWT) has gained reputation in signal processing and image/video compression. Wavelet transform decomposes a signal into a set of basis functions which

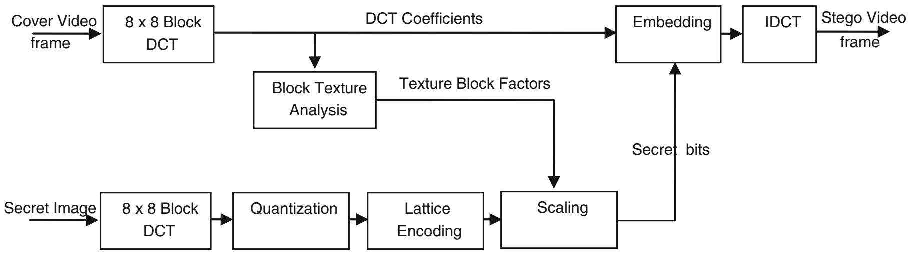


Fig. 8 Hiding process for [69]

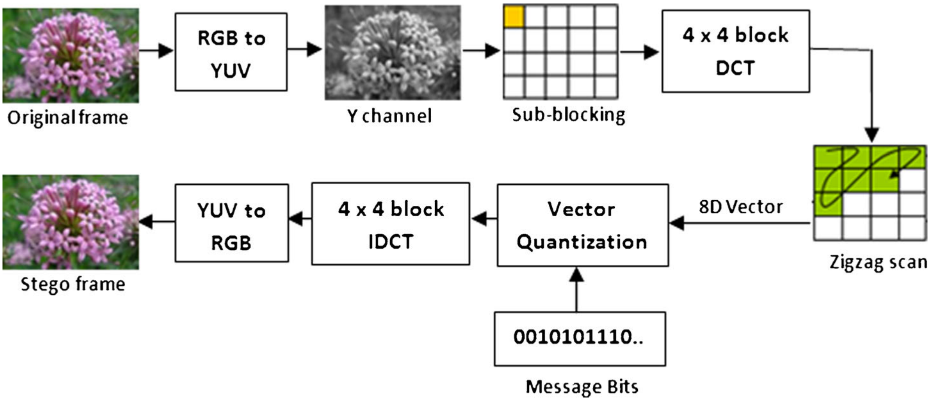


Fig. 9 Detailed hiding steps for [95]

are called wavelets. DWT provides a multi-resolution analysis that analyzes the signal at different frequencies giving different resolutions. The main advantage of DWT is temporal resolution. That is, it captures frequency as well as location information. An image/frame that is transformed with Haar wavelet transform [55] is broken down into four bands at each level of transformation. The first band is called the approximation band. It represents the input image after applying a low pass filter and compressing to half. The remaining three bands are called detail bands where high pass filter is applied. Figure 10 shows the 2D wavelet decomposition of a sample image.

The discrete wavelet transform has many advantages over DCT, particularly block-based DCT, such as: providing a multi-resolution description, allowing for better modeling of HVS. And the high-resolution sub-bands allow easy detection of features such as edges or textured areas in transform domain. In addition, DWT does not need to divide the input image into non-overlapping 2-D blocks, which decrease the blocking artifacts.

Similar to any transform, wavelet transform produces floating point coefficients even if the input data is integral [64]. In theory, these coefficients are used to perfectly reconstruct the original signal. But in practice, part of the signal is lost due to the finite arithmetic precision used. In an attempt to solve this problem, integer-to-integer wavelet transform appeared to allow perfect reconstruction of the original signal [9]. Thus, some video-steganography methods relied on the power of integer-to-integer wavelet transform. An example of these techniques was presented by Xu et al. [93]. They embedded the secret data in the motion component of video. And this is for two reasons: first, it is not greatly affected by compression and secondly, the human eyes are not sensitive to changes in motion areas. The algorithm works as follows: First motion component is calculated on a frame-by-frame basis. Then the calculated motion component undergoes two-level wavelet decomposition. After that, the secret bits are embedded into low frequency coefficients based on the values of coefficients in the three corresponding high frequency sub-bands. This is done to guarantee that the secret bits are embedded into large motion regions, maintaining a good video quality after embedding. The authors evaluated their work using PSNR and also with the steganalytic technique proposed in [20]. Two video sequences were embedded with secret bits of a text file for evaluation. Good average accuracy of the extracted data after MPEG-2 encoding was achieved ranging from 0.95 to 0.7. The only drawback of this algorithm is that it requires a video with large motion component otherwise the hiding capacity will drop.

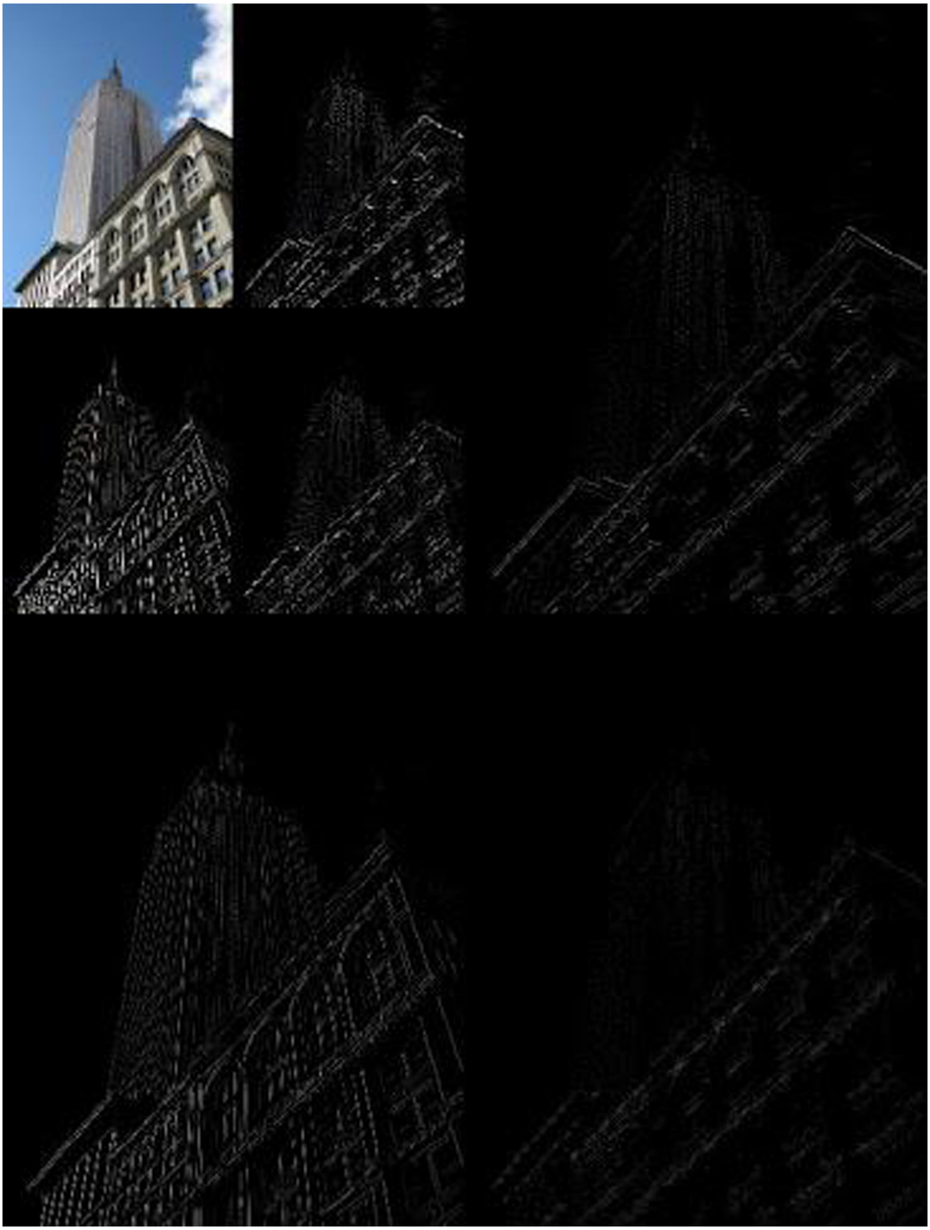


Fig. 10 Sample image transformed using Haar wavelet transform (http://code.google.com/p/wavelet1d/)

Another technique that used integer wavelet transform was presented by Abbass et al. [2], in which each frame of the cover video is decomposed into the three color components red, green and blue yielding three new video sequences. Then the discrete integer wavelet transform (DIWT) is applied on each sequence and the secret data is embedded in the least significant bits of the coefficients. After that, the inverse discrete integer wavelet transform (IDIWT) is applied and the three modified sequences are merged back into one stego-video.

The authors used 1D-DIWT performed across the time axis. Their results show that temporal 1-D DIWT is superior to LSB, 2D-DIWT and 3D-DIWT. And also their experiments showed that the blue frames have the least sensitivity with respect to the embedding distortion.

As discussed earlier, BPCS steganography [30] can be applied in the transform domain as well as the spatial domain. The idea was expanded by Noda et al. [58] in order to apply the BPCS steganography in the wavelet domain for hiding secret data in videos. They applied BPCS on videos encoded with wavelet based compression methods, namely 3D Set Partitioning in Hierarchical Trees (3D-SPIHT) encoded videos, and Motion-JPEG2000 encoded videos. These two compression techniques were selected as the wavelet coefficients in the transformed video are quantized into a bit-plane structure giving the possibility of applying BPCS steganography. Their results showed that 3-D SPIHT-BPCS is better than Motion-JPEG200GBPCS in terms of the embedding performance.

3.3 Adaptive techniques

Adaptive steganographic techniques are relatively a new class of embedding techniques. They are sometimes referred to as “Masking” [32] or “Statistics-aware embedding” [61]. An adaptive technique generally works by studying the statistical features of the cover before modification with the secret data. This process helps to identify the best regions to hide data [24] which are referred to as regions-of-interest ROI. In addition, this process can specify the amount of secret bits to hide depending on an adaptive capacity function.

Adaptive techniques can be considered special cases of the other classes. That is, in order to achieve better quality of the stego-video, the cover is adaptively modified according to some criteria. The famous LSB substitution method has an adaptive version which was used by Liao et al. [40]. The secret image extracted from the video stream itself, and then embedded in the background of the video frames. Figure 11 shows how their method works.

Video streams have multiple features that can be used for developing adaptive techniques. Temporal redundancy is one example. Sur et al. [84] based their algorithm on temporal redundancy. They select macro-blocks with low inter frame velocity and high prediction error as their ROI. Moreover, the number of DCT coefficients used for hiding is adaptively calculated based on the relative strength of the prediction error block. The algorithm is blind but it offers a very low hiding capacity.

Spatial properties are also important for adaptive techniques. Mansouri et al. [49] combined the use of spatial and temporal features of the video. They utilized a spatial key property which is texture. Qualified DCT coefficients of the I-frames and some motion vectors of P and B frames are their ROI. For I frames, quantized DCT coefficients are extracted and each 8×8 block is checked against a threshold to decide if it is suitable for hiding (highly textured or include edges). For qualified blocks, eight bits of secret data are embedded in eight quantized DCT coefficients that are determined by a secret key. Motion vectors of P and B frames above a certain threshold are used for hiding. For each qualified motion vector, two secret bits are embedded. This algorithm has a high hiding capacity as it uses both temporal and spatial features of the video stream.

Local contrast, color and areas of motion are the features chosen by Carli et al. [10] for developing a generic adaptive technique. Their method aims at maximizing both robustness and perceptual invisibility through selecting frame regions that are perceptually unimportant. A salience analysis is performed on each frame for finding these ROI. The salience analysis focuses on the three mentioned features. At the end, the three calculated features are weighed together to build an importance map to lead the hiding process. Once more, the hiding process can then be carried out using any specific algorithm.

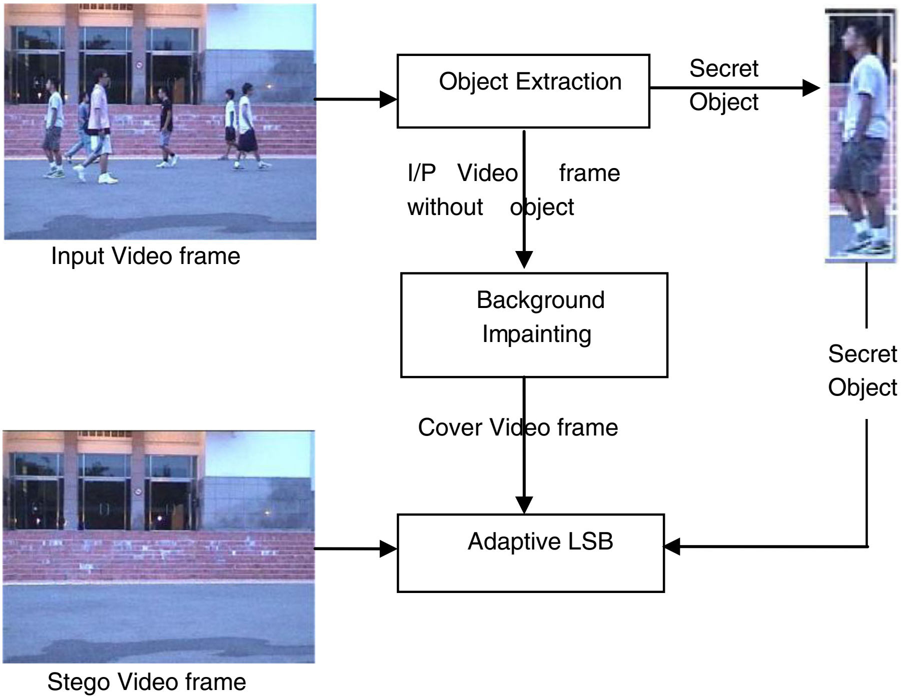


Fig. 11 Adaptive LSB [40] embedding process. The figure shows the output stego frame after extracting all the objects in the input frame and embedding them in the background

3.4 Format-based techniques

Various video formats were proposed in the literature to be used as cover objects. Format-based techniques are simply steganographic techniques designed for specific video formats. H.264/AVC is one of the latest compression standards for video. It provides high compression efficiency and it is well adapted for network transmission [66]. Multiple steganographic algorithms were designed to benefit from its structure. Ke et al. [36] utilized the Context Adaptive Variable Length Coding (CAVLC) characteristics to design a video steganographic technique. The code word of CAVLC is composed of six parts. “Total Coefficients and Trailing Ones”, “Trailing ones sign flag”, “Level prefix”, “Level suffix”, “Total Zeros” and “Run Before”. Modifying the “Total Coefficients”, “Trailing Ones”, “Total Zeros” or “Run Before” can cause de-synchronization of the code word, leading to problems in decoding video. So modifications caused by data hiding should maintain the stream structure. This leaves no space for the modifications except in levels coding. Changes should be done to high frequency coefficients not the low frequency ones, which if changed, will drop the video visual quality. As a result the designed algorithm use the “Trailing coefficient” symbols and the high frequency coefficients word for embedding data. Figure 12 shows the embedding algorithm. Various H.264 based techniques could be found in the literature, such as Liu et al. [46]. While Neufeld et al. [57] presented a study for the best data hiding locations in H.264 videos.

Flash video files (.FLV) are one of the popular video formats on the internet. They have simple structure and small size compared to other formats. An interesting technique related to this format was presented by Mozo et al. [54]. They utilized the format’s simple structure in

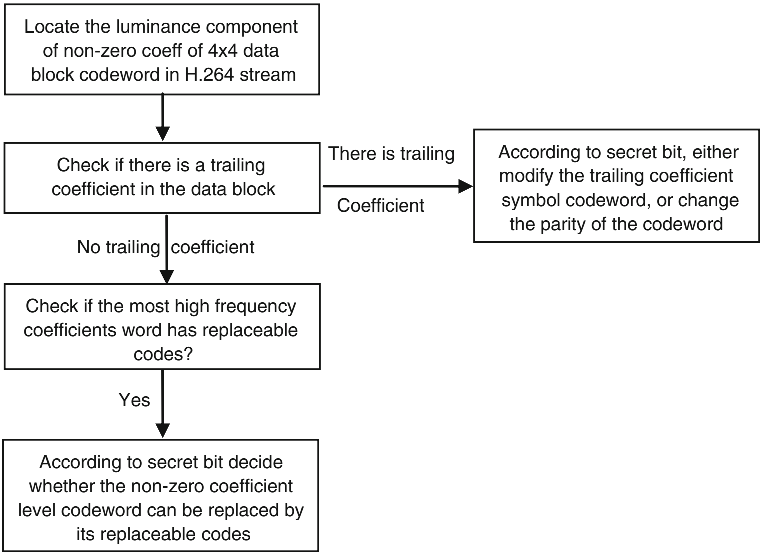

Locate the luminance component of non-zero coeff of 4x4 data block codeword in H.264 stream
Check if there is a trailing coefficient in the data block
There is trailing
Coefficient
According to secret bit, either modify the trailing coefficient symbol codeword, or change the parity of the codeword
No trailing coefficient
Check if the most high frequency coefficients word has replaceable codes?
Yes
According to secret bit decide whether the non-zero coefficient level codeword can be replaced by its replaceable codes

Fig. 12 H.264 data hiding algorithm for [36]

their algorithm. Their idea is to equally divide the secret message among the video tags of the entire file, adding them after each video tag in such a way that the actual video and audio tags are never modified or omitted. This keeps the video quality the same without any added distortion. This technique allows embedding unlimited size messages. However, the algorithm is just a naïve implementation. Additionally, it suffers from a number of drawbacks: the increase of the cover size with the size of the embedded message and the lack of tamper resistance.

3.5 Cover generation techniques

All traditional embedding methods discussed above use a certain cover object and apply a steganographic algorithm to hide secret data in it. In contrast, cover generation techniques synthesize an object to use it as a cover in a certain secret communication. This idea was implemented by Sampat et al. [73] for dynamic cover video generation. Their process involves the use of a secret key and the secret message itself for generating the cover video. The generation process uses a function X(A,D) where X is the function to generate the container file using the message, A is the number of samples required to hide the message and D is the message bits to be hidden. This method requires the use of a database of images to collect the required number of images necessary for the video generation. Figure 13 shows the required inputs and the pre-processing required. The advantage of this technique is the sustenance of steganalysis which does not provide the attacker with the original images. However the disadvantage is that if the selected sequence of images was irrelevant to each other, this may raise suspicion. As an improvement, the selected images may be put in the form of a slide show instead of a video while adding an appropriate audio to accompany the slideshow.

A summarization of the various discussed techniques is provided in Table 3 highlighting the pros and cons of each. In addition; whenever possible, the hiding capacity is calculated in terms of bits-per-pixel.

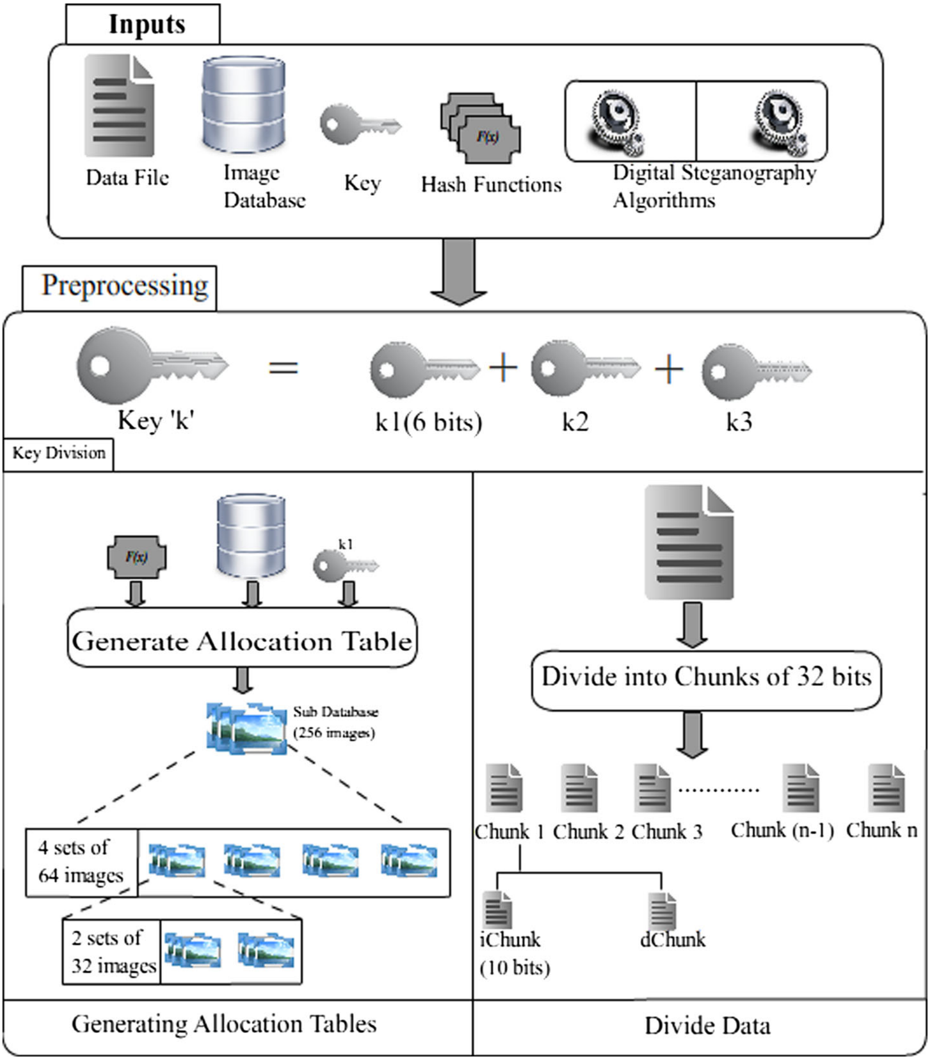


Fig. 13 Dynamic cover generation method: inputs and pre-processing [73]

4 Performance measures

The growth of video steganography raised a need for computational methods to evaluate the visual quality of the stego–video in a step towards evaluating the steganographic technique itself. Obviously, secret data embedding by any steganographic technique changes the quality of the original cover ranging from a slight alteration which is not noticeable by the human eye, to clear distortion that can be detected easily. Deciding whether the steganographic technique is perceptually transparent or not, needs standard metrics that can measure the alteration to the perceptual layout of the stego video. Basically, these metrics are used as an approximation to the human perception of stego-video quality.

The human vision test is the first type of measurement that has been found to measure the quality of steganographic objects after embedding the hidden data [25]. The human vision test

Table 3 Pros, cons and embedding capacity of the discussed techniques

Technique	Domain	Reference	Pros	Cons	Hiding capacity
Substitution-based (LSB)	Spatial	Singh et al. [80]	• Simple implementation. • Use only 1 LSB which keeps visual distortion to the minimum.	• Not robust against compression. • Not tamper resistant. • Low capacity compared to other LSB-based methods. Hides in independent frames.	1 bpp (gray)
	Spatial	Eltahir et al. [19]	• Simple implementation • Up to 33.3 % of each frame is utilized for data hiding. • Incorporate HVS features for enhancing the visual quality and capacity of LSB method.	• Not robust against compression. • Not tamper resistant. • Hides in independent frames.	8 bpp
	Spatial	Hu et al. [28]	• Hides an uncompressed secret video in the cover video with almost the same size. • Non uniform rectangular partitioning adds security as the partition codes are considered an encrypted version of the original secret frames.	• Inaccurate retrieval of the secret bits due to changing the original pixel values causing a problem in the decoding phase. • Increased visual distortion due to the use of 4 LSB for hiding. • Not robust against compression. • Not tamper resistant. • Hides in independent frames.	1.5 bpp
	Spatial	Hanafy et al. [22]	• Randomization of the secret message blocks. • Increased security due to the use of a secret key.	• Not robust against compression. • Hides in independent frames.	0.65 bpp
	Spatial	Shirali-Shahreza [77]	• Real time data hiding. • Can be used for broadcasting a secret message in a public place. • No storage space required. • Capable of hiding large messages in real time. • No Cover media available for use in attacks.	• Implementation requires a special device to be attached to the electronic billboard. • If frames are not photographed, then part of the secret message is lost. • The photographing process is sensitive to the environmental effects and needs an advanced camera.	N/A
		Channalli et al. [15]	• Inherits all advantages of the above method.	• Inherits all disadvantages of the above method.	1 bpp
Substitution-based (BPCS)	Spatial	Jalab et al. [30]	• The use of BPCS steganography increases the hiding capacity due to usage of multiple bit planes for hiding data. • Decreased color distortion as the method works with the YUV color space. • Flexibility in selecting the frame at which the embedding process starts.	• Not robust against compression. • Not tamper resistant. • Hides in independent frames.	N/A

Table 3 (continued)

Technique	Domain	Reference	Pros	Cons	Hiding capacity
			• More secure in term of avoiding the discovery of hidden data using the statistical techniques.		
Substitution-based (TPVD)	Spatial	Sherly et al. [76]	• A modified version of PVD, that provides increased capacity. • Hides secret bits in both vertical and diagonal edges of cover image in addition to the horizontal edges used in PVD. • Method benefits from video codec as I frames and motion vectors are used in the hiding process.	Can be attacked by Growing Anomalies [98].	I frames: 0.43 bpp B frames: 0.1 bpp P frames: 0.24 bpp
Transform Domain	DCT	Chae et al. [11]	• Robust against MPEG-2 • Decreased color distortion as the method works on Y component of the YUV color space. • Decreased visual distortion due to hiding in highly textured regions.	• Low capacity as 16 host video DCT blocks are required to embed one signature 8x8 DCT block. • The use of block DCT can result in blocking artifacts in the stego-video. • Although quantization of secret image decreases the amount of secret data, but it affects the quality of the retrieved image. • Hides in independent frames.	16 host video DCT blocks are required to embed one signature 8x8 DCT block.
		Yang et al. [95], Shou-Dao et al. [79]	• High bitrate data hiding. • Robust against H.264 and MPEG-4 compression. • Decreased color distortion as the method works on Y component of the YUV color space. • Tamper resistant. • Useful in practical applications such as captioning, video-in-video and speech-in-video.	• There is a trade-off between robustness to compression and visual distortion. • Data hidden within different types of frames have different levels of robustness against compression due to the different coding strategies of I, P and B frames. • The use of block DCT can result in blocking artifacts in the stego-video. • Hides in independent frames.	1 bit per 4*4 DCT block
		Xu et al. [94]	• Decreased distortion due to the use of motion vectors with large magnitudes. • Robust against video processing manipulations (frame adding, frame dropping, re-ordering some adjacent frames). • Method benefits from video codec as I frames and motion vectors are used in the hiding process.	• Hiding capacity is affected by the redundant embedding of the secret message and the embedding of control information in I frames.	0.57 bits/P macro-block and 1.71 bits/B macro-block
	DWT	Xu et al. [93]	• Robust against MPEG-2 compression.		

Table 3 (continued)

Technique	Domain	Reference	Pros	Cons	Hiding capacity
			• Method benefits from video specific properties due to the use of motion component for hiding. • Hide in motion component, while the human eyes are more sensitive to the change in still regions. Use of integer wavelet transform.	• Hiding capacity drops if the used cover video doesn't have large motion component.	Large motion: 440 byte/frame. small motion: 40 byte/frame. Frame size: 352× 288
		Abbass et al. [2]	• Achieves zero bit error rate (BER) between the original and the recovered data • Algorithm has low computational complexity compared with other DWT techniques due to using 1D-DWT • Use of integer wavelet transform	• Hides in independent frames.	N/A
		Noda et al. [58]	• Method benefits from the bit-plane structure of the quantized wavelet coefficients and applies BPCS steganography. • Comparative study between 3-D SPIHT-BPCS steganography and Motion-JPEG2000-BPCS steganography.	• Restricted to wavelet-compressed videos.	Embedding in 1 bit-plane: 0.13 bit/pixel Embedding in 2 bit-planes: 0.2 bit/pixel
Adaptive	Spatial	Liao et al. [40]	• Adaptive and simple data hiding method.	• Not robust against compression. • Not tamper resistant.	N/A
	DCT	Sur et al. [84]	• Embeds data in macroblocks with low inter-frame velocity and high prediction error. • Adaptively specify the number of DCT coefficients to be used for hiding based on the strength of the prediction error block. • Robust with respect of the quantization error because embedding is done after quantization. • Method benefits from video codec as P and B macroblocks are used in the hiding process.	• Low hiding capacity	0.0093 bits
		Mansouri et al. [49]	• Adaptively embeds data in I frame DCT blocks based on the texture. • Adaptively embeds data in motion vectors of P and B frames based on their magnitudes.	• Restricted to MPEG videos.	Average capacity of I frame: 5,520 P frame: 382 B frame: 168

Table 3 (continued)

Technique	Domain	Reference	Pros	Cons	Hiding capacity
			• High hiding capacity due to the use of both temporal and spatial features of the cover. • Method benefits from video codec as I, P and B frames are used in the hiding process.		Frame size: 352× 288
	General	Carli et al. [10]	• Use of local contrast, color and motion areas for adaptively finding best regions for hiding. • Increased visual quality due to hiding in perceptually unimportant regions. • Generic technique can be used with any appropriate data hiding method.	• Applying the algorithm before starting the data hiding method itself adds an overhead to the whole process in terms of time and complexity.	N/A
Format-based	DCT	Ke et al. [36]	• Algorithm maintains the bitrate. • Decreased visual distortion due to working on high frequency coefficients. • Method benefits from the H.264 video codec. • Method does not require decoding and re-encoding the cover video.	• Secret message may not be extracted correctly if the embedded message length was ruined. • Capacity is proportional to the number of data blocks with trailing coefficients and non-zero coefficient.	1 bit per each 4x4 residual data block
	Spatial	Mozo et al. [54]	• Unlimited size data can be hidden without affecting the video quality. • FLV files are relatively small and very popular on internet, and have simple understandable structure.	• Causes original file size to change. • To avoid file size changing, FLV file must be compressed first before embedding the data leading to visible distortions. • Not robust against compression. • Not tamper resistant.	Unlimited
Cover Generation	General	Sampat et al. [73]	• Dynamically generates a new cover video by using an images database. • Steganalysis is more difficult as the original video does not exist. • Generic technique can be used with any appropriate data hiding method.	• Raises suspicion if the video is constructed from irrelevant sequence of images.	N/A

is done with the naked eye, by surveying some persons who are asked to examine the original and the stego videos, then they report if they noticed any distortion or alteration in the perceptual vision of the stego video by providing a score. This score is known as Mean Opinion Score (MOS) [92]. However, it is highly subjective and hence is inefficient, not reliable, and expensive in terms of preparation time, running and human resources needed. As a result, other objective quality metrics evolved.

Objective quality metrics are algorithms that can numerically estimate the quality of the video, thus predicting the viewers MOS. These metrics can be divided into two different approaches: error-based approach and structural distortion approach. Error-based approach depends on the fact that there is a direct relation between the decrease in perceptual quality and the visibility of the error signal so it measures different aspects of the error signal depending on their visibility to the human eye. On the other hand, structural distortion approaches measures the distortion by using the structural distortion in the video. It is based on the assumption that HVS focuses on extracting the structural information from the viewing field. As a result, the distortion increases as the structural information decreases. In this case, the distortion is not related to the errors [88].

In this section, we will review mean square error-based metrics, video quality metric and moving pictures quality metric, as examples of error-based metrics. While Structural Similarity Index and General Video Quality Model, are reviewed as examples of structural distortion metrics.

Mean Square Error (MSE) represents the accumulated squared error between original and stego-frames. The square root of the MSE represents the Root Mean Square Error (RMSE). A very close metric is the Signal -to-Noise Ratio (SNR) which measures the amount of noise corruption to the original signal. Similarly, the Peak Signal-to-Noise Ratio (PSNR) calculates the highest SNR between two images/frames. As the PSNR increases, the quality of the stego object is better. An enhancement to PSNR is the Weighted PSNR (WPSNR). It considers that the human eye is less sensitive to changes in textured areas than in smooth areas. Therefore, the PSNR is weighted by an HVS parameter called noise visibility function (*NVF*) [56]. Notice that, all of the above metrics are measured in decibel (dB). The formulas used to calculate these metrics are provided in Table 4.

Because of their simplicity and low computational complexity, PSNR and MSE are widely used as quality metrics. However, they do not accurately model the perceptual quality as their calculation does not incorporate any modeling of the Human Visual System. Also these metrics were initially designed for images, so they might not be optimal when applied on videos. Video Quality Metric VQM [60] and Moving Pictures Quality Metric MPQM [87] are two error-based metrics specially designed for videos.

Video Quality Metric (VQM) measures the perceived video quality by measuring how much the video is affected by various types of distortion. VQM is developed by The Institute for Telecommunication Science (ITS) and has been adopted by The American National Standards Institute (ANSI) as an objective video quality standard [89]. Having the original and the stego videos, VQM can be calculated in four steps. First, the processed video is calibrated and then a mathematical function is used to extract quality features that indicate perceptual changes in the spatial and temporal properties of the video regions. Third, the extracted features from the processed video are compared against those from the original video and the quality parameters are calculated. Finally, the parameters from the previous step are combined into a single result.

On the other hand, Moving Pictures Quality Metric (MPQM) takes into consideration two human vision characteristics namely contrast sensitivity and masking [89]. Contrast sensitivity refers to the fact that the human eye detects a certain signal only if its contrast is greater than

Table 4 Some error-based quality metrics and their formulas

Quality Metric	Formula	Parameters
Mean Square Error (MSE)	$\mathrm{MSE} = \frac{1}{m*n}\sum_{i=0}^{m}\sum_{j=0}^{n}\left(A_{ij}-B_{ij}\right)^2$	A_{ij}: one pixel in the cover image B_{ij}: one pixel in the stego-image m*n: represent height and width of the image.
Root Mean Square Error (RMSE)	$\mathrm{RMSE} = \sqrt{\frac{1}{m*n}\quad\sum_{i=0}^{m}\sum_{j=0}^{n}\left(A_{ij}-B_{ij}\right)^2}$	A_{ij}: one pixel in the cover image B_{ij}: one pixel in the stego-image m*n: represent height and width of the image.
Signal-to-Noise Ratio (SNR)	$\mathrm{SNR} = 10 * \log_{10}\frac{\sum_{i=1}^{n}\sum_{j=1}^{m}\left(A_{ij}\right)^2}{\sum_{i=1}^{n}\sum_{j=1}^{m}\left(A_{ij}-B_{ij}\right)^2}$	A_{ij}: one pixel in the cover image B_{ij}: one pixel in the stego-image
Peak Signal-to-Noise Ratio (PSNR)	$\mathrm{PSNR} = 10 * \log_{10}\frac{(Max)^2}{\frac{1}{m*n}\sum_{i=0}^{m}\sum_{j=0}^{n}\left(A_{ij}-B_{ij}\right)^2}$ $\mathrm{PSNR} = 10 * \log_{10}\frac{(Max)^2}{MSE}$	A_{ij}: one pixel in the cover image B_{ij}: one pixel in the stego-image m*n: represent height and width of the image. Max: represent the maximum value of the colors which is 255
Weighted Peak Signal-to-Noise Ratio (WPSNR)	$\mathrm{WPSNR} = 10\log_{10}\left[\frac{max(p(x,y))^2}{MSE\times NVF}\right]$ $\mathrm{NVF} = \mathrm{NORM}\left(\frac{1}{1\times\delta_{block}{}^2}\right)$	δ_{block}: standard deviation of luminance of the block of pixels. MSE: Mean Square Error NVF: Noise Visibility Function

some threshold. Masking is related to the human vision response to a combination of signals. The original and stego frames are decomposed into perceptual channels. Then contrast sensitivity and masking are measured on a channel-base. Finally, all channels measurements are combined together giving a rate from 1 to 5 where 1 is the worst and 5 is the best. The only drawback of MPQM is that it does not consider the chrominance, but that was addressed in color MPQM (CMPQM) [86].

Another category of video specific metrics is called structural distortion metrics. An example of this type of metrics is the Structural Similarity Index (SSIM) presented by Zhou Wang [90]. The method is built upon the fact that the human eye can cleverly extract structural information rather than extracting errors. Calculating SSIM requires the calculation of the means, variances and covariance of the original and distorted frames. This calculation is done on each 8xs8 pixel block of the original frame, and the distorted frame. Using the calculated block SSIM, the next step involves calculating a quality index for each frame. Then in the final step, the total quality of the video is calculated as a whole by weighing the sum of the frame quality indices. The weight values used for each frame are dependent on the motion in that frame.

Another example of structural distortion metrics is the General Video Quality Model ($\mathrm{VQM_G}$) [60]. $\mathrm{VQM_G}$ is a general purpose quality model that can be used for videos with various bit rates, frame rates and resolutions. It was developed by The National Telecommunications and Information Administration (NTIA), and has been standardized by The American National Standards Institute (ANSI) [60]. The model is based on seven independent parameters; each represents a certain quality feature of the video. For each and every feature, a filter is first applied on the original and distorted video to enhance some property important for quality such as edge information, then the features are extracted, and finally, a perceptibility threshold is applied to the extracted features. The $\mathrm{VQM_G}$ is calculated as a linear combination of the seven parameters as follows. The model gives output starting from zero, which is the best case where no distortion is perceived, and as the distortion increases, the output value increases as well. The formulas used to calculate these metrics are provided in Table 5.

Although, VQM, MPQM, SSIM and VQM$_G$ are metrics specially designed for video, they are not standardized yet. Some efforts are done in the road to standardization such as [1].

5 Steganalysis: an overview

Steganography and steganalysis are in a never ending battle. Whenever a good steganographic technique is developed, another steganalysis technique is also developed trying to defeat it [91]. Steganalysis is the art and science of detecting secret messages hidden using steganography [33]. Once there is evidence that a message is hidden, the goal of steganography is defeated even if the message was not extracted. Although steganographic techniques may be visually transparent to the human eyes, attacks on them are still possible. Any embedding process inevitably leaves traces in the stego-object and alters some of its properties which introduce unusual characteristics and some degradation in terms of quality. Hence, steganalysis can be classified into two categories [12]: passive steganalysis and active steganalysis. Passive steganalysis detect the presence or absence of hidden message or identify the embedding algorithm used [82]. While active steganalysis change, extract or destroy the hidden message or extract some of its attributes such as message length [98].

Table 5 some structural distortion metrics and their formulas

Quality Metric	Formula	Parameters
Structural Similarity Index (SSIM)	SSIM for a block: $SSIM_i(t) = \frac{4\mu_i(t).\mu_i{}'(t)cov\ _i(t)}{\left(\mu_i{}^2(t)+\mu_i{}'^2(t)\right).\left(\sigma_i{}^2(t)+\sigma_i{}'^2(t)\right)}$	
	Frame quality index Q(t): $Q(t) = \frac{\sum_{i=1}^{R} w_i(t).SSIM_i(t)}{\sum_{i=1}^{R} w_i(t)}$	$w_i(t)$: a weight which depends on the local luminance. $SSIM_i(t)$: Block SSIM
	SSIM for the entire video: $\text{SSIM} = \frac{\sum_i W(t).Q(t)}{\sum_i W(t)}$	
General Video Quality Model (VQM$_G$)	VQM= −0.2097 * si_loss +0.5969 * hv_loss +0.2483 * hv_gaint +0.0192 * chroma_spread −2.3416 * si_gain +0.0431 * ct_ati_gain +0.0076 * chroma_extreme	si_loss: Detects loss of spatial information (e.g. blurring). hv_loss: Detects a shift of edges from horizontal and vertical to diagonal orientation. hv_gain: Detects a shift of edges from diagonal to horizontal and vertical orientation (e.g. blocking). si_gain: Measures improvements of quality caused by edge sharpening or enhancement. chroma_spread: Detects changes in the spread of color samples distribution. chroma_extreme: Detects severe localized color impairments. ct_ati_gain: Measures perceptibility of spatial impairments in dependence of the amount of motion as well as perceptibility of temporal impairments in dependence of the amount of spatial data.

Different active steganalysis methods exists, some of them are specific to certain steganographic algorithms meaning that they attack a certain steganographic technique but does not work with other techniques [83, 98], while others are general attacks that can be performed in order to destroy the message hidden using any steganographic technique. An example of specific steganalytic methods is the one proposed by Zaker et al. [98] where a statistical method is designed to estimate the amount of secret bits hidden using TPVD. Another method was introduced by Su et al. [83] which detect the hidden information using motion-vector-based steganographic algorithms.

This section does not dive into the details of different steganalysis methods or its classification. Instead, we will discuss steganalysis from the point of view that help designing a robust steganographic technique. Therefore, we will review some steganalysis attacks that should be tested for evaluating the strengths and weaknesses of the designed steganographic algorithm.

In fact, after designing a steganographic technique, it should be tested to know its strengths and weakness. The designed technique should be tested against several image processing attacks, and also against any known steganalysis technique specific to the designed technique. Here we suggest some tests and attacks used frequently in literature, for testing any steganographic algorithm.

Perceptual transparency analysis the invisibility of a data hiding algorithm is the first and most important requirement, since the strength of steganography lies in the concealment of the communication. Thus the moment that the human eye can detect that some changes happened to the video, the algorithm is defeated. The simplest type of testing is the subjective testing. It is done by comparing the original video frames and the stego video frames with the naked eyes [93, 95]. For measuring the perceptual transparency, there are numerous metrics available which have been discussed in the previous section. One of the most widely used metrics is the PSNR [11, 22, 28, 49, 76, 93–95]. A minimum PSNR value of 38 dB is adopted as the quality requirement for the stego images/frames [76].

Histogram analysis is another simple and effective way for testing a steganographic algorithm effect on the stego frames. It is done by simply comparing the histogram of the frame before and after embedding to know the change in the pixels color distribution caused by the steganographic algorithm used. This test was utilized by the authors in [8, 19, 30, 76].

Bit error rate (BER) it indicates the amount of secret message bits that survived and was extracted successfully from the stego video. BER is defined as the ratio between the count of wrong extracted bits and the count of original message bits. The equation of BER = Count of Error Bits/Count of original message bits. BER was used in [79, 95].

Robustness against compression: Since an uncompressed video have very large size, it must be compressed before transmission. This led to great emphasis on testing the robustness of stego videos against compression. This is usually done by compressing the stego videos using different compression techniques and at various compression rates, in order to know the survival rate of the hidden bits. Flexibility to MPEG-2 encoding was tested by the authors in [93]. They calculated the ratio between the correctly extracted bits and the total number of secret message bits at three different bitrates to know the flexibility of their algorithm against compression.

Robustness against image/video manipulation a stego video may intentionally or accidentally undergo changes by image or video processing operations. The effect of common image processing attacks such as translation, rotation, cropping, blurring and addition of noise should be tested [16]. Common video processing attacks such as frame adding and frame dropping should also be tested [94].

Reporting the results of the above attacks and measures for a certain steganographic technique gives a clear honest view of the strengths and weaknesses of the designed method.

6 Conclusion

This paper presents a comprehensive review of video steganographic techniques. Difference between steganography, cryptography, and watermarking were discussed. An overview of steganography using different cover types was presented and special attention was paid to video steganography and its applications. Various categorizations of the existing techniques were illustrated. We adopted a categorization according to the domain of embedding, in which methods are categorized into three categories: Spatial domain techniques, transform domain techniques, and other techniques. Techniques belonging to each domain were discussed and comparisons between those techniques were presented highlighting their advantages and disadvantages. Furthermore, popular image and video quality metrics available in the literature were discussed. Finally, steganalysis was surveyed from the point of view that improves the design of good steganographic systems. Based on this review, the following recommendations may help interested researchers in video steganography.

Integration of steganography and cryptography Encrypting the secret message before hiding in the cover adds another security layer to the hidden message. In case the steganography failed and the message existence was detected, the attacker still has to break the encryption to know the hidden message.

Blind data retrieval Blind retrieval refers to the ability to extract the secret message without requiring the use of the original cover in the extraction process. If the data hiding technique does not support blind extraction, this will require sending the original cover twice which will be suspicious. Thus blind extraction increases the algorithm security.

Working with YUV color space The YUV color space de-correlates the dependencies of the RGB color components into one luminance component and two chrominance components. It is used extensively in video compression techniques such as MPEG. Furthermore, the human eyes are more sensitive to changes in the chrominance components than to the luminance one. So utilizing the Y-component for embedding minimizes color distortion that results in stego object [30].

Design steganographic techniques that are specifically adapted for videos video signal is a highly correlated signal. This correlation origin from both spatial correlation and temporal correlation [74]. Most video steganographic techniques in the literature treat each video frame independently. So it is more significant to design video steganographic techniques that benefit from the video codec and the available properties such as motion vectors, motion components, etc.

Avoid using videos with smooth homogeneous background [17]: studies shows that the human visual system can easily spot artifacts in areas of homogeneous color [30]. So the use of textured visually complex videos and videos with high motion is recommended to help conceal the hidden data.

Designing steganographic techniques for compressed videos Videos mostly exist in a compressed format, so that they can be transferred easily and do not require a large bandwidth. Techniques that hide data in uncompressed videos have to take into consideration how to make the embedded data survive video compression. So it is more significant to design video data hiding techniques that operate on compressed videos. And in such case, the technique should maintain the compressed stream bitrate.

Embedding data in the DWT domain Spatial domain techniques are simple, easy to implement and have high hiding capacity. On the other side they are vulnerable to even small changes. In addition, they are neither tamper resistant nor robust to compression, directing the emerging techniques towards embedding in the transform domain [48], Since DWT has a number of advantages over DCT as discussed before, making it more eligible for this type of data hiding.

Using adaptive techniques for data hiding Adaptive techniques are special cases of the spatial or transform domain techniques. They interact with the cover object in a smart way in order to either maximize its hiding capacity, or minimize the distortion caused by embedding. This can be achieved in various ways such as using a dynamic capacity function, applying some adjustment algorithm to adjust the stego object and minimize the effect of changed data, or analyzing the cover to find the best regions for hiding data. Up till now, adaptive techniques have no known statistical vulnerabilities [17]. So it is an appealing sort of data hiding that still needs more exploration.

An ideal and perfect video steganographic algorithm should provide large hiding capacity, high imperceptibility, robustness, and tamper resistance. But such an algorithm does not exist in reality. All the reviewed algorithms had strengths and weaknesses that depend on the adopted algorithm and the type of the application. So it is important to ensure that one should use the appropriate algorithm for given application.

References

1. (2008) Objective Perceptual Multimedia Video Quality Measurement in the Presence of a Full-Reference, ITU-T Rec. J. 247
2. Abbass AS, Soleit EA, Ghoniemy SA (2007) Blind video data hiding using integer wavelet transforms. Ubiquit Comput Commun J 2(1)
3. Ahsan K, Kundur D (2002) Practical data hiding in TCP/IP. In: Proc. of Workshop on Multimedia Security at ACM Multimedia
4. Alattar AM, Alattar OM (2004) Watermarking electronic text documents containing justified paragraphs and irregular line spacing. In: Proc. of SPIE 685–695
5. Al-Frajat AK, Jalab HA, Kasirun ZM, Zaidan AA, Zaidan BB (2010) Hiding data in video file: an overview. J of Appl Sci (Faisalabad) 10(15):1644–1649
6. Anderson RJ, Petitcolas FAP (1998) On the limits of steganography. IEEE J Sel Areas Commun 16(4): 474–481
7. Bailey K, Curran K (2006) An evaluation of image based steganography methods. Multimed Tools Appl 30(1):55–88
8. Balaji R, Naveen G (2011) Secure data transmission using video Steganography. In: IEEE International Conference on Electro/Information Technology (EIT) 1–5
9. Calderbank AR, Daubechies I, Sweldens W, Yeo B-L (1997) Lossless image compression using integer to integer wavelet transforms. In: Proceedings of International Conference on Image Processing 596–599
10. Carli M, Campisi P, Neri (2006) A Data hiding driven by perceptual features for secure communications. In: International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies (ICN/ICONS/MCL) 85–85

11. Chae JJ, Manjunath BS (1999) Data hiding in video. In: Proceedings of International Conference on Image Processing (ICIP 99) 311–315
12. Chandramouli R, Memon ND (2003) Steganography capacity: A steganalysis perspective. In: Proceedings of SPIE 173–177
13. Chang K-C, Chang C-P, Huang PS, Tu T-M (2008) A novel image steganographic method using tri-way pixel-value differencing. J Multimed 3(2):37–44
14. Chang F-C, Hang H-M, Huang H-C (2007) Layered access control schemes on watermarked scalable media. J VLSI Signal Process Syst Signal Image Video Technol 49(3):443–455
15. Channalli S, Jadhav A (2009) Steganography an Art of hiding data. Int J Comput Sci Eng (IJCSE) 1(3): 137–141
16. Cheddad A, Condell J, Curran K, Mc Kevitt P (2009) A skin tone detection algorithm for an adaptive approach to steganography. Signal Process 89(12):2465–2478
17. Cheddad A, Condell J, Curran K, Mc Kevitt P (2010) Digital image steganography: survey and analysis of current methods. Signal Process 90(3):727–752
18. Das R, Tuithung T (2012) A novel steganography method for image based on Huffman Encoding. In: 3rd National Conference on Emerging Trends and Applications in Computer Science (NCETACS) 14–18
19. Eltahir ME, Kiah LM, Zaidan BB, Zaidan AA (2009) High rate video streaming steganography. In: International Conference on Future Computer and Communication (ICFCC 2009) 672–675
20. Fridrich J, Goljan M, Du R (2001) Detecting LSB steganography in color, and gray-scale images. Multimed IEEE 8(4):22–28
21. Hamid N, Yahya A, Ahmad RB, Al-Qershi OM (2012) Image steganography techniques: an overview. Int J Comput Sci Secur (IJCSS) 6(3):p168–p187
22. Hanafy AA, Salama GI, Mohasseb YZ (2008) A secure covert communication model based on video steganography. In: Military Communications Conference (MILCOM 2008) 1–6
23. Handel TG, Sandford Ii MT (1996) Hiding data in the OSI network model. In: Proceedings of the First International Workshop on Information Hiding 23–38
24. Herrera-Moro DR, Rodríguez-Colín R, Feregrino-Uribe C (2007) Adaptive Steganography based on textures. In: 17th International Conference on Electronics, Communications and Computers (CONIELECOMP'07) 34–34
25. Hmood AK, Kasirun ZM, Jalab HA, Alam GM, Zaidan AA, Zaidan BB (2010) On the accuracy of hiding information metrics: counterfeit protection for education and important certificates. Int J Phys Sci 5(7): 1054–1062
26. Horng S-J, Rosiyadi D, Fan P, Wang X, Khan MK (2013) An Adaptive Watermarking Scheme for e-government Document Images. Multimed Tools Appl. doi:10.1007/s11042-013-1579-5
27. 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 and Image Represent 24(7):1099–1105
28. Hu S, KinTak U (2011) A Novel Video Steganography Based on Non-uniform Rectangular Partition. In: IEEE 14th International Conference on Computational Science and Engineering (CSE) 57–61
29. 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(16):3379–3396
30. Jalab H, Zaidan AA, Zaidan BB (2009) Frame selected approach for hiding data within MPEG video using bit plane complexity segmentation. J Comput 1(1):108–113
31. Jia Y, Lin W, Kassim AA (2006) Estimating just-noticeable distortion for video. IEEE Trans Circ Syst Video Technol 16(7):820–829
32. Johnson NF, Jajodia S (1998) Exploring steganography: seeing the unseen. IEEE Comput 31(2):26–34
33. Johnson NF, Jajodia S (1998) Steganalysis: The investigation of hidden information. In: Information Technology Conference 113–116
34. Katzenbeisser S and Petitcolas F (2000) Information Techniques for Steganography and Digital Watermarking. Artec House
35. Kawaguchi E, Eason RO (1999) Principles and applications of BPCS steganography. In: Photonics East (ISAM, VVDC, IEMB) International Society for Optics and Photonics 464–473
36. Ke N, Weidong Z (2013) A Video Steganography Scheme Based on H.264 Bitstreams Replaced. In: Software Engineering and Service Science (ICSESS), 2013 4th IEEE International Conference on 447–450
37. Kim Y-W, Moon K-A, Oh I-S (2003) A text watermarking algorithm based on word classification and inter-word space statistics. In: Proc. of the Seventh International Conference on Document Analysis and Recognition (ICDAR'03) 775–779
38. Langelaar GC, Lagendijk RL (2001) Optimal differential energy watermarking of DCT encoded images and video. IEEE Trans Image Process 10(1):148–158
39. Latif A (2013) An adaptive digital image watermarking scheme using fuzzy logic and tabu search. J Inform Hiding and Multimed Signal Process 4(4):250–271

40. Liao Y-C, Chen C-H, Shih TK, Tang NC (2009) Data hiding in video using adaptive LSB. In: Joint Conferences on Pervasive Computing (JCPC) 185–190
41. Lie W-N, Lin T-I, Lin C-W (2006) Enhancing video error resilience by using data-embedding techniques. IEEE Trans Circ Syst Video Technol 16(2):300–308
42. Lin W-H, Horng S-J, Kao T-W, Chen R-J, Chen Y-H, Lee C-L, Terano T (2009) Image copyright protection with forward error correction. Expert Syst Appl 36(9):11888–11894
43. 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(5):746–757
44. Lin W-H, Wang Y-R, Horng S-J (2009) A wavelet-tree-based watermarking method using distance vector of binary cluster. Expert Syst Appl 36(6):9869–9878
45. Lin W-H, Wang Y-R, Horng S-J, Pan Y (2009) A blind watermarking method using maximum wavelet coefficient quantization. Expert Syst Appl 36(9):11509–11516
46. Liu Y, Li Z, Ma X, Liu J (2013) A robust data hiding algorithm for H.264/AVC video streams. J Syst Softw 86:2174–2183
47. Low SH, Maxemchuk NF, Brassil JT, O'Gorman L (1995) Document marking and identification using both line and word shifting. In: Proc of Fourteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Bringing Information to People.(INFOCOM'95) 853–860
48. Maniccam SS, Bourbakis N (2004) Lossless compression and information hiding in images. Patern Recognit 37(3):475–486
49. Mansouri J, Khademi M (2009) An adaptive scheme for compressed video steganography using temporal and spatial features of the video signal. Int J Imaging Syst Technol 19(4):306–315
50. Mat Kiah ML, Zaidan BB, Zaidan AA, Mohammed Ahmed A, Al-bakri SH (2011) A review of audio based steganography and digital watermarking. Int J Phys Sci 6(16):3837–3850
51. Mazurczyk W, Ml S, Szczypiorski K (2011) Retransmission steganography and its detection. Soft Comput J 15(3):505–515
52. McKeon RT (2007) Strange Fourier steganography in movies. In: IEEE International Conference on Electro/Information Technology 178–182
53. Mercuri RT (2004) The many colors of multimedia security. Commun of the ACM 47(12):25–29
54. Mozo AJ, Obien ME, Rigor CJ, Rayel DF, Chua K, Tangonan G (2009) Video steganography using flash video (FLV). In: Instrumentation and Measurement Technology Conference (I2MTC'09) 822–827
55. Mulcahy C (1997) Image compression using the Haar wavelet transform. Spelman Sci and Math J 1(1):22–31
56. Navas KA, Sasikumar M (2011) Image fidelity metrics: future directions. IETE Tech Rev 28(1)
57. Neufeld A, Ker AD (2013) A study of embedding operations and locations for steganography in H.264 video. In: Proc. SPIE, Media Watermarking, Security, and Forensics 8665
58. Noda H, Furuta T, Niimi M, Kawaguchi E (2004) Application of BPCS steganography to wavelet compressed video. In: International Conference on Image Processing (ICIP'04) 2147–2150
59. Petitcolas FAP, Anderson RJ, Kuhn MG (1999) Information hiding-a survey. Proc IEEE 87(7):1062–1078
60. Pinson MH, Wolf S (2004) A new standardized method for objectively measuring video quality. IEEE Trans Broadcast 50(3):312–322
61. Provos N, Honeyman P (2003) Hide and seek: an introduction to steganography. Secur & Priv IEEE 1(3): 32–44
62. Rabah K (2004) Steganography-the art of hiding data. Inf Technol J 3(3):245–269
63. Raja, K.B., Chowdary, C.R., Venugopal, K.R. & Patnaik, L.M. (2005) A secure image steganography using LSB, DCT and compression techniques on raw images. In: Proceedings of IEEE 3rd International Conference on Intelligent Sensing and Information Processing, 170–176.
64. Rao RS, Karthik MV, Nagla S (2012) Wavelet transform based image compression. Int J Eng Res Appl (IJERA) 2(6):1509–1514
65. Raphael AJ, Sundaram V (2010) Cryptography and steganography-a survey. Int J Comput Tech Appl 2(3): 626–630
66. Richardson IEG (2003) H.264 and MPEG-4 video compression: video coding for next-generation multimedia. Wiley, Chichester
67. Risca VI (2001) DNA-based steganography. Cryptologia 25(1):37–49
68. Ritchey PC, Rego VJ (2012) A context sensitive tiling system for information hiding. J Inf Hiding and Multimed Sig Process 3(3):212–226
69. Robie DL, Mersereau RM (2002) Video error correction using steganography. EURASIP J Adv Signal Process 2(1900):164–173
70. Rosiyadi D, Horng S-J, Fan P, Wang X, Khan MK, Pan Y (2012) An efficient copyright protection scheme for e-government document images. IEEE Multimed 19(3):62–73
71. Rosiyadi D, Horng S-J, Suryana N, Masthurah N (2012) A comparison between the hybrid using genetic algorithm and the pure hybrid watermarking scheme. Int J Comput Theory and Eng (IJCTE) 4(3):329–331

72. Sakib MN, Alam SB, Sazzad ABMR, Shahnaz C, Fattah SA (2011) A Basic Digital Watermarking Algorithm in Discrete Cosine Transformation Domain. In: Second International Conference on Intelligent Systems, Modelling and Simulation (ISMS) 419–421
73. Sampat V, Dave K, Madia J, Toprani P (2012) A Novel Video Steganography Technique using Dynamic Cover Generation. In: National Conference on Advancement of Technologies – Information Systems & Computer Networks (ISCON – 2012), Proceedings published in Int J of Comput Appl (IJCA)
74. Shang Y (2007) A new invertible data hiding in compressed videos or images. In: Third International Conference on Natural Computation (ICNC) 576–580
75. Sharda S, Budhiraja S (2013) Image steganography: a review. Int J of Emerg Technol Adv Eng 3(1): 707–710
76. Sherly AP, Amritha PP (2010) A Compressed Video Steganography using TPVD. Int J of Database Manag Syst 2 (3). doi:5121/ijdms.2010.2307 67
77. Shirali-Shahreza M (2006) A new method for real-time steganography. In: 8th International Conference on Signal Processing
78. Shirali-Shahreza MH, Shirali-Shahreza M (2006) A new approach to Persian/Arabic text steganography. In: 5th IEEE/ACIS International Conference on Computer and Information Science, and 1st IEEE/ACIS International Workshop on Component-Based Software Engineering, Software Architecture and Reuse (ICIS-COMSAR) 310–315
79. Shou-Dao W, Chuang-Bai X, Yu L A High Bitrate Information Hiding Algorithm for Video in Video.
80. Singh S, Agarwal G (2010) Hiding image to video: a new approach of LSB replacement. Int J Eng Sci and Technol 2(12):6999–7003
81. 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 (SACI'07) 241–244
82. Su Y, Zhang C, Wang L, Zhang C (2008) A new video steganalysis based on mode detection. In: International Conference on Audio, Language and Image Processing (ICALIP 2008) 1507–1510
83. Su Y, Zhang C, Zhang C (2011) A video steganalytic algorithm against motion-vector-based steganography. Signal Process 91(8):1901–1909
84. Sur A, Mukherjee J (2006) Adaptive data hiding in compressed video domain. In: Computer Vision, Graphics and Image Processing 738–748
85. Tak UK, Tang Z, Qi D (2009) A non-uniform rectangular partition coding of digital image and its application. In: International Conference on Information and Automation (ICIA'09) 995–999
86. Van den Branden Lambrecht CJ (1996) Color moving pictures quality metric. In: Proceedings of International Conference on Image Processing 885–888
87. Van den Branden Lambrecht CJ, Verscheure O, Technology (1996) Perceptual quality measure using a spatiotemporal model of the human visual system. In: Electronic Imaging: Science & Technology 450–461
88. Vranjes M, Rimac-Drlje S, Zagar D (2007) Objective video quality metrics. In: 49th Int. Symp. ELMAR 45–49
89. Wang Y (2006) Survey of objective video quality measurements. EMC Corp Hopkinton, MA, 1748
90. Wang Z, Lu L, Bovik AC (2004) Video quality assessment based on structural distortion measurement. Signal Process Image Commun 19(2):121–132
91. Wang H, Wang S (2004) Cyber warfare: steganography vs. steganalysis. Commun the ACM 47(10):76–82
92. Webster AA, Jones CT, Pinson MH, Voran SD, Wolf S (1993) Objective video quality assessment system based on human perception. In: IS&T/SPIE's Symposium on Electronic Imaging: Science and Technology, International Society for Optics and Photonics 15–26
93. Xu C, Ping X (2007) A steganographic algorithm in uncompressed video sequence based on difference between adjacent frames. In: Fourth International Conference on Image and Graphics (ICIG) 297–302
94. Xu C, Ping X, Zhang T (2006) Steganography in compressed video stream. In: First International Conference on Innovative Computing, Information and Control (ICICIC'06) 269–272
95. Yang M, Bourbakis N (2005) A high bitrate information hiding algorithm for digital video content under H. 264/AVC compression. In: 48th Midwest Symposium on Circuits and Systems 935–938
96. Yilmaz A, Alatan AA (2003) Error concealment of video sequences by data hiding. In: Proc. of International Conference on Image Processing (ICIP) 3:II 679–682
97. Yuhong Wang CZ, Sukesh Kaithaapuzha visual masking model implementation for images & video

98. Zaker N, Hamzeh A (2012) A novel steganalysis for TPVD steganographic method based on differences of pixel difference histogram. Multimed Tools Appl 58(1):147–166
99. Zhang W, Cheung SC, Chen M (2005) Hiding privacy information in video surveillance system. In: Proc. of the 12th IEEE International Conference on Image Processing 868–871
100. Zhang J, Li J, Zhang L (2001) Video watermark technique in motion vector. In: Proceedings of XIV Brazilian Symposium on Computer Graphics and Image Processing 179–182

Menna Sadek Currently works as a teaching assistant at Basic Sciences department at the Faculty of Computers & Information Science, Ain Shams University, Egypt. She graduated in 2009. Her main research interests are Steganography, encryption and Security.

Amal Khalifa Currently working as an assistant professor of Scientific Computing at Faculty of Computers & Information Science, Ain Shams University, Egypt. She graduated in 2000 and worked as a teaching assistant for a number of undergraduate courses till 2004. Meanwhile, she got her MSc degree in the field of *Information Hiding in Digital Images*. In 2005 she was granted a 2 years research scholarship in University of Connecticut, USA. She earned her PhD degree in 2009 in the area of *High performance Computing*. Her main research interests are Steganography, computational biology, parallel computing, encryption and Security.

Prof. Mostafa Gadal-Haqq M. Mostafa received a B.Sc. (Honor) in 1984 in Physics, a M.Sc. in 1989 and a Ph.D. in 1996, in Computational Physics from the Faculty of Science, Ain Shams University, Cairo, Egypt. He is a Professor of Computer Science at the Faculty of Computer and Information Sciences, Ain Shams University. He worked as a research scientist at the Oak Ridge National Lab (ORNL), USA, in the period from 1993 to 1995, and he joined the Department of Electrical and Computer Engineering, University of Louisville, USA, in the period from 1998 to 2000. He also joined the Faculty of Computer Science and Engineering, Taibah University, Madinah, Saudi Arabia in the period from 2001 to 2009. He has published more than 30 scientific articles in international and local journals and conferences. He has co-authored two books (in Arabic) in the field of computer science. His research interests includes: Computer Vision, Pattern Recognition, Medical Image Analysis, Arabic Optical Character Recognition, Speech Processing, Bioinformatics, and Information Security.