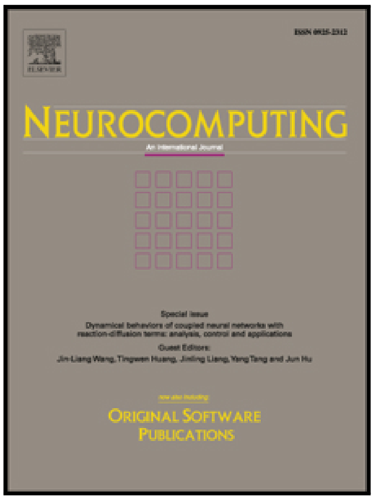
Accepted Manuscript



Video Steganography: A Review

Yunxia Liu , Shuyang Liu , Yonghao Wang , Hongguo Zhao ,
Si Liu

PII: S0925-2312(18)31260-8
DOI: https://doi.org/10.1016/j.neucom.2018.09.091
Reference: NEUCOM 20084

To appear in: *Neurocomputing*

Received date: 1 August 2018
Revised date: 14 September 2018
Accepted date: 29 September 2018

Video Steganography: A Review

Yunxia Liu[1]*, Shuyang Liu[2], Yonghao Wang[3], Hongguo Zhao[1], Si Liu[1]

1. College of Information Science and Technology, Zhengzhou Normal University, Zhengzhou, China
2. School of mathematics and statistics, Lanzhou University, Lanzhou, China
3. Computing and Digital Technology, Birmingham City University, Birmingham,UK

E-mail address: liuyunxia0110@hust.edu.cn

Abstract Video steganography is becoming an important research area in various data hiding technologies, which has become a promising tool because not only the security requirement of secret message transmission is becoming stricter but also video is more favored. In this paper, according to the embedded position of secret message, video steganography is divided into three categories: intra-embedding, pre-embedding and post-embedding. Intra-embedding methods are categorized according to the video compression stages such as intra-prediction, motion vectors, pixels interpolation, transform coefficients. Pre-embedding methods are manipulated on the raw video, which can be classified into spatial and transform domains. Post-embedding methods are mainly focused on the bitstreams, which means the procedure of embedding and extraction of video steganography are all manipulated on the compressed bit stream. Then we introduce the performance assessment for video steganography and the future popular video steganography including H.265 video steganography, robust video steganography and reversible video steganography. And challenges are finally discussed in this paper.

***Keywords*: *Data hiding; Video steganography, Visual quality, Embedding capacity, Robustness, Intra-embedding, Pre-embedding, Post-embedding*.

1. Introduction

Video steganography is a branch of data hiding, which is a technique that embeds message into cover contents and is used in many fields such as medical systems, law enforcement, copyright protection and access control, etc. [1].Since human visual system are less sensitive to the small changes of digital medias, especially for digital video, video steganography is a technique which hides message into a video and conceals the fact of the transmission. And it has become more popular recently because of two main reasons: Along with the fast development of computer applications, the security problem in information field is becoming more and more serious. Video is an electronic medium which can be more eligible than other multimedia because of the booming of powerful sharing/transmission tools of digital video contents and its size.

Three main important factors should be considered in any successful steganography system: imperceptibility, robustness and embedding capacity [2].

Imperceptibility is closely related to the safety of steganography methods concealing the secret message into the embedded video. The high imperceptibility means a low modification rate and good visual quality of the embedded video [2]. And the steganography algorithm that contains a high imperceptibility will reduce attacker suspicion of finding hidden message and will be quite difficult to detect by steganalysis tools, and any distortion to the cover data after the embedding process occurs will increase the attention of attackers [3]. In video steganography, imperceptibility is the perceptual similarity between the original and embedding video, and evaluated as a visual distortion caused by embedding modifications. To improve the imperceptibility, many video steganography methods have used lots of methods such as quantization transform coefficients [17-23], predictions modes [15-16], and motion vectors [56-65], etc. to enhance the performance of imperceptibility.

Robustness is the second prerequisite which measures the steganography method's strength against attacks in video steganography. The reason of the consideration of robustness is that the embedded message sometimes cannot survive from various intentional or unintentional attacks, such as network transmission, packet loss, video clipping and scaling operations [4]. And the figures 1-2 present the intentional and unintentional attacks, respectively. The algorithm is robust when the receiver can extract the secret message correctly without any errors. To improve the robustness, many techniques have been made in video steganography, such as BCH code [18], secret sharing [20-21], and histogram distribution constrained [72], etc. The robustness is critical to the quality of the video steganography method, as the literature in [102] depicted, high efficient steganography algorithms should be robust against both signal processing and adaptive noises. To improve the evaluation precisely, the survival rate is that all the embedded bits are divided by the embedded bits retrieved without error is used to measure robustness [3].

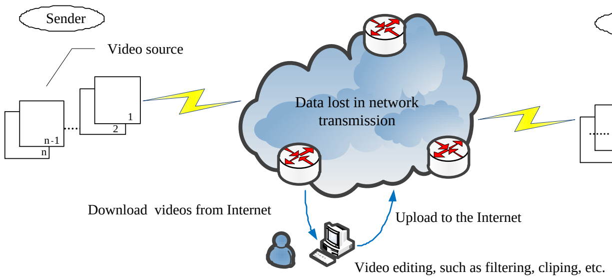


Fig. 1 Unintentional attacks

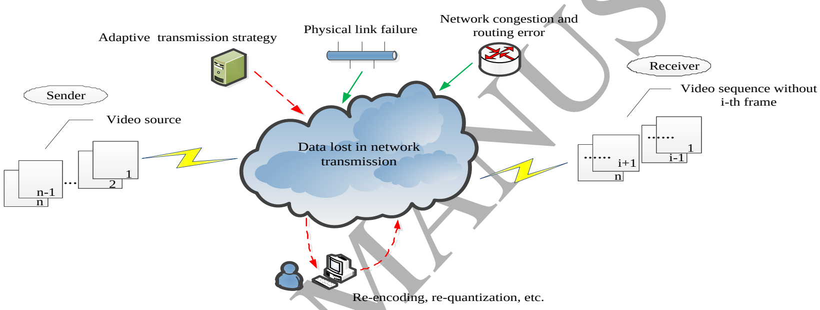


Fig. 2 Intentional attacks

Embedding capacity is the third fundamental prerequisite and is defined as the sum of secret message that can be embedded into the digital video. The higher embedding capacity means the more secret message can be embedded. However, higher embedding capacity could lead to the higher risk for the decrease of visual quality and increment of bit-rate for the embedded video. In traditional steganography methods, embedding capacity and imperceptibility of embedded video are inter conditioned, and the imperceptibility is affected by embedding capacity. So the imperceptibility of video steganography should be taken into account when the method has higher embedding capacity. To increase the embedding capacity with the high imperceptibility, many state-of-the-art technologies have been presented in the steganography methods, which are based on H.264 and respectively utilized the combination of the prediction modes and DST coefficients [19-21], pixel interpolation [52], motion estimation [57], etc. During the evaluation of steganography methods, the imperceptibility should be considered prior to embedding capacity because we can get the embedding video that the message needed because of the infinite video sequences [2].

There is an exchange-off in the imperceptibility, robustness and embedding capacity. In the video steganography method, if either the robustness or embedding capacity increases, the imperceptibility will reduce.

Recently, numerous video steganography methods have been proposed. The research interests not only focused on the traditional fields (e.g., DST transform domain) but also combined the technologies of the emerging fields, such as artificial intelligence [5-9]. However, there exists a problem that the survey of video steganography lacks sufficient articles. A comprehensive introduction and analysis of the video steganography methods has been provided in this paper. In addition, recommendations and future directions are also suggested to enhance the development of video steganography methods.

The goal of this paper is to make a review on video steganography research, highlight their contributions, and discuss about their challenges. The remainder of this paper is organized as follows. Section 2 introduces the theoretical concepts of the most popular algorithms in video steganography. Section 3 introduces the performance assessment metric for video steganography. And section 4 is the future popular video steganography, including H.265 video steganography, robust video steganography and reversible video steganography. And conclusions are in Section 5.

2. Video Steganography Method

Up to date, with the rapid advancement of Internet and multimedia technologies, the digital videos have become a popular field for data hiding. The infinite video sequences also provide a massive amount of redundancy space for embedding secret message in video steganography.

The existing video steganography algorithms can be divided into three categories according to the embedding position: the pre-embedding (the message embedding position is the raw video domain), the intra-embedding (the message embedding position is the compressed domain) and the post-embedding (the message embedding position is the bitstream domain). The performances of the evaluation criteria of the algorithm should be considered: imperceptibility, robustness, embedding capacity, algorithm complexity, etc.

2.1 Video steganography techniques based on intra-embedding

Intra-embedding combines the embedding process of video coding and syntax elements such as intra-prediction, motion estimation and DCT coefficients: the sender embeds secret message into the process of video, as shown in Fig.3.

The intra-embedding steganography method has greater application and gained more attention because the video is usually transmitted or stored after compression coding. At present, the popular video coding standards H.26X and MPEG-X have high compression ratio, and the video data redundancy has been removed to a great extent after compression coding, which makes it more difficult to embed more data into the compressed video stream [10-12]. In the literatures, most of the intra-embedding steganography method can be selected via part of the video coding structure, including Discrete Cosine/Sine Transform (DCT/DST) [3, 13-27], intra prediction [28-41], motion estimation [42-57, 65], etc., to embed message.

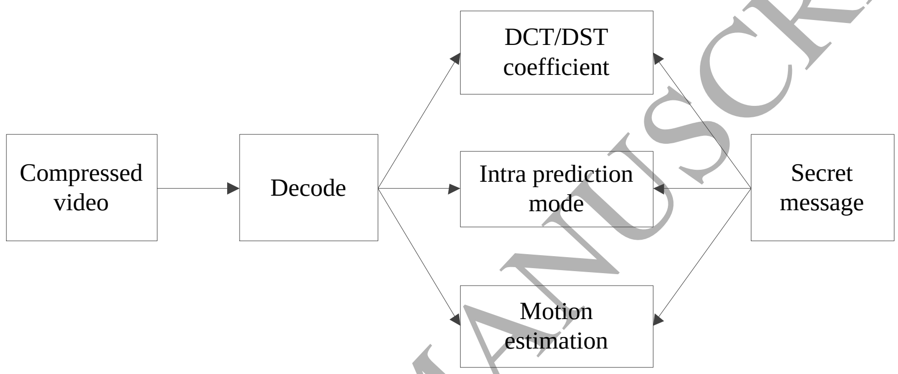


Fig.3 Intra-embedding video steganography

DCT/DST and Quantized DCT/DST (QDCT/QDST) coefficients of the luminance are good candidates to embed secret message because of their low, middle and high frequency coefficients [20]. If the message is embedded into the non-quantized DCT coefficients, the part of the embedded message will be lost after it's been quantified; and if the message is embedded into the quantized DCT coefficients, it can skip the quantization process and can adapt to the lossy compression coding, but it can impact on the visual effect. Video steganography technique based on DCT is one of the most popular methods in H.264 (H.264/AVC), and the existing H.264 video steganography methods based on DCT coefficient usually chooses quantized DCT coefficients to embed message. Fig.4 shows the message is embedded into the quantized DCT coefficients and Fig. 5 shows the message is extracted from the quantized DCT coefficients.

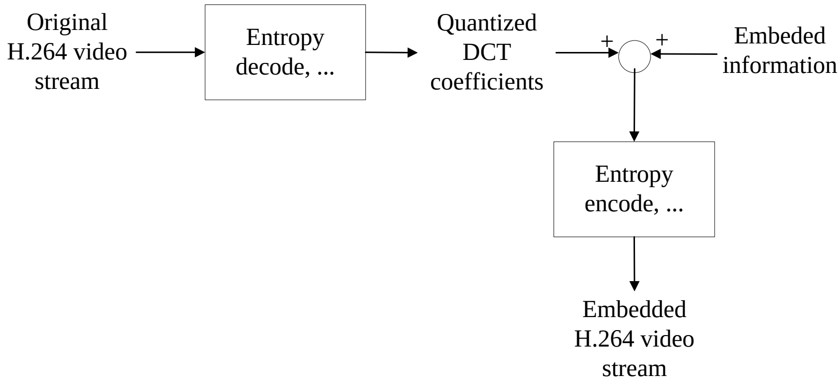


Fig.4 The message embedded into the quantized DCT coefficients

.

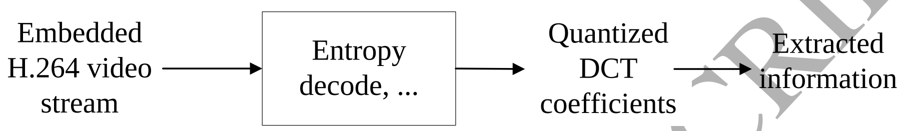


Fig.5 The message extracted from the quantized DCT coefficients

In addition, H.264 has the similar transform manner the coding of the residual samples to H.265 (H.265/HEVC), which means that two-dimensional transforms of DCT can be computed by applying 1-D transforms in the horizontal and vertical directions. In order to reserve the computing precision and orthogonality, the core transform of the DCT coefficients is computed by approximating and scaling DCT basic functions with integer values. The integer transform based on 4×4 block is shown in equation (1), where $Y_{4\times4}$ is the matrix of unscaled DCT coefficients corresponding to the residual block $X_{4\times4}$. In particular, for the transform block size of 4×4 in H.265, the DST integer transform which derived from DCT is applied and shown in (2).The difference between DCT and DST is that DST transform only use to 4×4 blocks in H.265 and DCT can be applied for the other blocks transform in H.264 and H.265 [94].

$$Y = (\mathrm{C}XC^T) \tag{1}$$

Where

$$C = \begin{Bmatrix} 1 & 1 & 1 & 1 \\ 2 & 1 & -1 & -2 \\ 1 & -1 & -1 & 1 \\ 1 & -2 & 2 & -1 \end{Bmatrix}$$

$$Y = (HXH^T) \tag{2}$$

Where

$$H = \begin{Bmatrix} 29 & 55 & 74 & 84 \\ 74 & 74 & 0 & -74 \\ 84 & -29 & -74 & 55 \\ 55 & -84 & 74 & -29 \end{Bmatrix}$$

This section will discuss some H.264 Video steganography techniques based on quantized DCT coefficients. [13] employed a human visual model based on 4×4 block discrete cosine transform to embed the secret message into quantized Alternating Current (AC) DCT coefficients of the luminance residual blocks. The method has not handled the intra-frame distortion drift in H.264. [14] handled the intra-frame distortion drift and proposed an algorithm which embeds secret message into the quantized Direct Current (DC) DCT coefficients of the luminance residual blocks. But the algorithm is detectable and non-blind. [16] developed a group of paired-coefficients which could effectively avoid the intra-frame distortion drift. [3] improved the performance of [16] and proposed an robust without distortion drift steganography algorithm based on BCH, which can correct the error bits caused by network transmission, packet loss, video-processing operations, various attacks, etc. [17] improved [3] and proposed a robust steganography scheme for H.264 by using Shamir's (t, n)-threshold secret sharing and BCH to improve the robustness of the embedded message. [19-22]further provided reversible video steganography methods based on the utilization of BCH code and shamir secret sharing, respectively.

Based on H.265/H.264 intra-prediction coding, the code blocks are encoded by a number of intra-prediction modes. In H.265 codec, the number of intra prediction modes are 35 for each 64×64, 32×32, 16×16, and 8×8 blocks. Fig.6 depicts the 33 angel prediction orientations. And the H.264 codec supports 9 prediction modes for 4×4 blocks and 4 prediction modes for 16×16 blocks. Since the prediction modes play a key role in the compressed procedure, there are a number of methods which utilized the prediction modes to embed message.

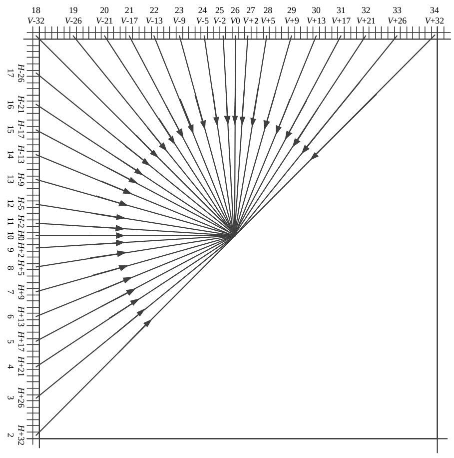


Fig.6 33 angle prediction modes of H.265

Among the steganography algorithms for H.264 based on the intra prediction mode (IPM) [28-37], [28] modified the intra prediction mode based on the mapping between the secret message and the prediction mode. [30] improved the best prediction mode matching method by using the least Lagrangian cost. [31] established a mapping between the message and intra prediction mode with matrix coding. [32] proposed an algorithm based on [31] and utilized an embedding/extracting matrix. Zhang et al. [34] developed a high security adaptive embedding algorithm by using STC (Syndrome-Trellis Code). To resist the detection from [36], [37] introduced the minimizing the “embedding distortion” defined according to SAD (Sum of Absolute Difference).

Motion estimation is used for steganography by modifying motion vector or adjusting the motion vector search process. In the earlier work [42-45], motion vector (MV) was used to hide message usually by directly modifying motion estimation, which is relatively simple, but the embedding performance is not good enough. [47] began to embed secret message by adjusting the parity of the horizontal component and the vertical component. [48] applied matrix coding and phase angle to improve the video quality. [49] inspired by Fridrich et al [50]’s perturbed quantization (PQ) steganography, a technique called perturbed motion estimation (PME) is introduced to minimize the embedding impacts. [52] embedded the message in another way by modifying the search range of motion. [54] designed a MV-distortion function by joining the spatial distortion change (SDC) and the prediction error change (PEC) together, and the two-layered Syndrome Trellis Code (STC). [55] is further utilized to achieve high security level. [56] created N-dimensional motion vector space to get high embedding efficiency. [57] introduced a specific decoded reference frame to overcome the distortion accumulation effects. To resist the steganalysis [51, 58-64] like AoSO and SPOM, [65] further proposed the most suitable CMV (Candidate MV) to guarantee the local optimality of modified motion vectors.

Intra-embedding is easy to allocate the hidden message to the video, and it can get better subjective visual quality and stronger anti-attack ability, but it relies on a specific video codec, and the application scope of the video steganography algorithm is limited to the corresponding codec.

2.2 Video steganography techniques based on pre-embedding

The sender embeds secret message into the non-compressed video stream and then compresses the video, and the receiver decodes the received compressed video and extracts the secret message from the original video. Video steganography based on pre-embedding mainly considers the video sequence as a set of frames, as shown in Fig.7. Pre-embedding video steganography techniques consists of spatial [66-77] and transform domain technique [78-85].

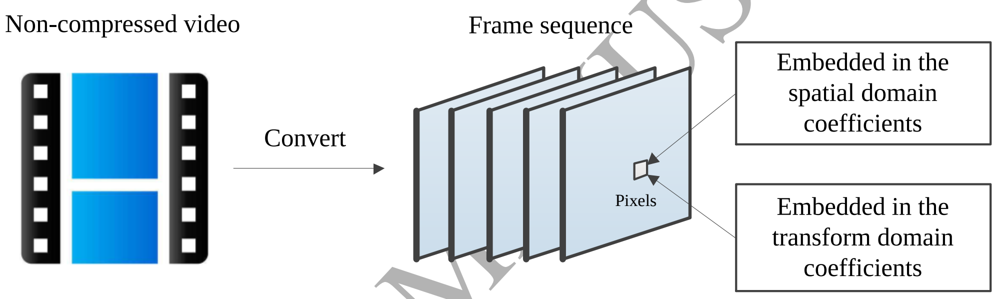


Fig.7 Pre-embedding video steganography

As for the Video steganography techniques based on the spatial domain, [71] embedded secret data in the carrier AVI video file in least significant bit (LSB). The method is simple and has a high embedding capacity, but the robustness is insufficient and hard to resist steganalysis. [72] further proposed a secured hash-based LSB technique (Hash-LSB). In [73], Hash-LSB with the RSA algorithm is implemented to provide a more secure steganography method. [76] developed a blind steganography method based on histogram techniques with an appropriate pixel selection mechanism. [77] introduced a histogram distribution constrained (HDC) scheme to resist H.246 video compression. [74] used region of interest (ROI) to embed the secret message. This method is limited in embedding capacity as only single video frame is considered for embedding stage. [75] combined the Kanade-Lucas-Tomasi (KLT) tracking and Hamming codes (15, 11). The encoded secret message is embedded using an adaptive LSB substitution method in the ROIs of video frames. This method shows good embedding capacity, but the complexity of the operation is also high.

As for the Video steganography techniques based on the transform domain, [79] used face detection and face tracking algorithms to the cover videos in the wavelet domain in order to identify the facial regions of interest. [80] developed a blind adaptive method where human skin regions are regarded as the ROI. The discrete wavelet transform(DWT) coefficients in the skin tone areas guarantee the relatively big amplitude signals which have strong noise immunity. [81] introduced the Hamming and BCH codes to improve the security. The message is embedded into DCT coefficients of each Y, U, and V planes excluding DC coefficients. The visual quality is not very ideal. [82] used DCT and DWT coefficients in combination to enhance the security of hidden message and minimize distortions to maintain better video quality. [83] improved the video steganography method in DWT and DCT domains based on the multiple object tracking (MOT) algorithm and error correcting codes. Motion-based MOT algorithm is implemented on host videos to distinguish the regions of interest in the moving objects. The method showed good security and robustness against various attacks.

The pre-embedding method is independent of the specific video coding process and does not affect the use of the existing standard codec; it can use a variety of message hiding techniques and strategies based on the images [76-77]. However, after video codec the secret message will inevitably have some loss, which is very bad for the extraction and detection of the hidden message [72]. And it takes more time and is not very efficient [84].

2.3 Video steganography techniques based on post-embedding

The post-embedding video steganography algorithm is that the sender directly embeds secret message into compressed bitstream, and the receiver extracts secret messages directly from the received embedded compressed video bit stream. It is not practical to embed the whole bit stream because of the constraints of format compliance and computational complexity. Alternatively, many video steganography algorithms consider the coding structure and embed only a fraction of video data.

H.264 supports two types of entropy (bitstream) coding modules. Context-adaptive variable length coding (CAVLC) [86-88] is supported in H.264 baseline profile and context-adaptive binary arithmetic coding (CABAC) [89-92] is supported in H.264 main profile. CAVLC is a lower complexity but less efficient entropy coder than CABAC [93].The post-embedding process based on H.264/AVC is shown in Fig.8.

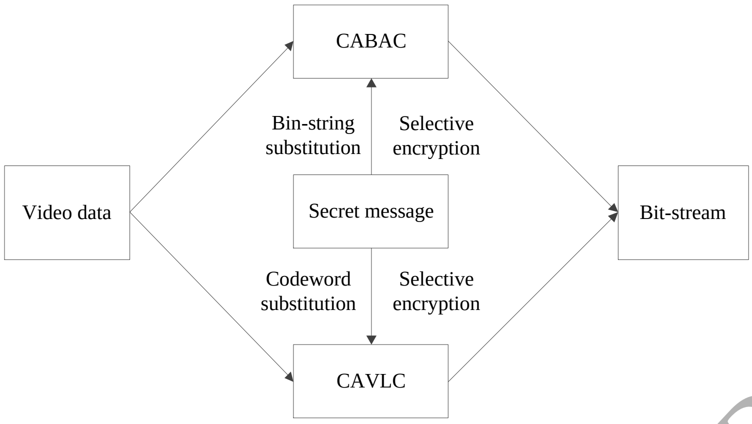


Fig.8 Post-embedding video steganography

Based on CAVLC, the literature [86] proposed a video steganography based on H.264 by Selective Encryption (SE). SE is performed in the CAVLC module of video codec, and CAVLC is converted to an encryption cipher using permutation of equal length codes from a specific variable length coding (VLC) table. [87] used the advanced encryption standard (AES) algorithm to improve SE process. To solve the encrypting problem of nonzero coefficients, [88] proposed a tunable scheme that intra prediction modes and the sign bits of motion vectors were encrypted together.

Based on CABAC, [91] introduced a data-hider to embed the message into partially encrypted H.264/AVC videos by using a CABAC bin-string substitution technique without accessing the plaintext of the video content. Since bin-string substitution is carried out on the residual coefficients, the quality of the decrypted video is satisfactory. [92] improved [91], the encryption of luma prediction modes is designed in addition to residual encryption and motion vector encryption in order to significantly improve the structural deterioration.

The post-embedding method does not need the process of complete decoding and re-encoding, and the computational complexity is low [86]. It will not affect the normal operation of the existing video compression codec, and make the best use of the existing hardware resources [88]. However, because of the operation on video compression bit streams, the video compression codec system is highly dependent. The algorithm design must take into account the factors such as bit stream format, synchronization and transmission conditions [89]. For example, because the limitation of compressed bit rate, the amount of data embedded in video is also limited. Thus the robustness of the format conversion operation is poor [92].

3. Performance Assessment for video steganography

The main goal of video steganography is to conceal the secret message into the digital video, so the visual quality of the embedded video would be changed ranging from a slight distortion to a severe distortion. In order to evaluate the imperceptibility is acceptable or not, several assessment metrics have been used for the evaluation of visual quality, especially for Pick Signal to Noise Ratio (PSNR) and Structural Similarity (SSIM). PSNR is a common assessment metrics which represents the difference between the original and cover videos [16, 25]. In order to be consistent with performance of HVS, SSIM is also used in video steganography [23]. Because PSNR is based on the error between corresponding pixels and the visual characteristics of the human eye are not taken into consideration, the evaluation result is inconsistent with the subjective feeling of the person video quality evaluation based on error sensitivity. And because SSIM is mainly used to measure the structural integrity of frame, the frame is generally divided by a sliding window, where the sliding window is generally a Gaussian window, and the mean, variance and covariance of each window are calculated by Gaussian weighting. Then the calculation of SSIM method is slightly complex, and its value can better reflect the subjective feelings of human eyes. The PSNR and SSIM are defined as follows:

$$PSNR = 10 \times Log_{10}(\frac{MAX_A^2}{MSE})(dB) \tag{3}$$

$$MSE = \frac{\sum_{i=1}^{a}\sum_{j=1}^{b}\sum_{k=1}^{c}[A(i,j,k)-B(i,j,k)]^2}{a \times b \times c}$$

Where *A* and *B* represent the original and embedded frames, *a* and *b* represent the resolution of the specific videos, *c* refer to the RGB color components. *MAX* represents the highest pixel value in frame A.

$$SSIM = \frac{(2\mu_A\mu_B + C_1)(2\sigma_A + C_2)}{(\mu_A^2 + \mu_B^2 + C_1)(\sigma_A^2 + \sigma_B^2 + C_2)} \tag{4}$$

Where *A* and *B* represent the original and embedded frames, μ_A and σ_A represent the mean and standard deviation values of pixels in frame *A*, C_1 and C_2 refer to a fixed value, respectively.

As mentioned before, the robustness is one important attribute for video steganography method. And the assessment metric indicates that the embedded message whether can be retrieved from the receiver or not. Similarity (*Sim*) and bit error rate (*BER*) have been used to evaluate the robustness performance of video steganography. The Sim and BER can be defined as follows:

$$Sim = \frac{\sum_{i=1}^{a}\sum_{j=1}^{b}[M(i,j)\times \hat{M}(i,j)]}{\sqrt{\sum_{i=1}^{a}\sum_{j=1}^{b}M(i,j)^2}\times\sqrt{\sum_{i=1}^{a}\sum_{j=1}^{b}\hat{M}(i,j)^2}} \tag{5}$$

$$BER = \frac{\sum_{i=1}^{a}\sum_{j=1}^{b}[M(i,j)\oplus \hat{M}(i,j)]}{a\times b} \tag{6}$$

where $M(i,j)$ and $\hat{M}(i,j)$ are the original and obtained message, $a\times b$ is the size of the embedded message.

The performance of embedding capacity is also a major factor that directly affects the evaluation of the steganography method. The Hiding ratio (*HR*) [83] has been used to evaluate for the embedding capacity in steganography methods and calculated in the following formula:

$$HR = \frac{Size\ of\ \ the\ embedded\ \ message}{Video\ size}\times 100\% \tag{7}$$

Table I provides the performance of intra-embedding, pre-embedding and post-embedding methods in terms of visual quality, robustness and embedding capacity. It can be seen from Table I that the intra-embedding methods have a high visual quality, but the embedding capacity is small. In addition, the performance of robustness in these methods are not always considered, which was easily detected by various steganography methods. Embedding capacity and robustness are properties that need to be further enhanced in the future. The pre-embedding methods based on spatial/transform domain generally have relatively good embedding capacity and visual quality, but the main challenge is its robustness to resist the vulnerability of any unexpected modification including compression, format change, etc. Therefore, such methods must improve the robustness against compression, signal processing, noises, etc. The post-embedding methods modify entropy elements based on CAVLC or CABAC and achieve the robustness performance. However, the visual quality of the post-embedding methods is not very good when compared to the intra-embedding methods. It can be seen that there still exist improvement in terms of visual quality, embedding capacity and robustness.

Table I: Embedding capacity, video quality and robustness comparison of the video steganography method classifications

Method	Intra-/pre-/post-embedding	HR	PSNR	robustness
Algorithm in[[16]	Intra-embedding	0.10%	40.74dB	×
Algorithm in[[20]	Intra-embedding	0.09%	46.35dB	√
Algorithm in [27]	Intra-embedding	1.04%	37.00dB	×
Algorithm in[40]	Intra-embedding	1.62%	40.25 dB	×
Algorithm in[56]	Intra-embedding	0.03%	36.79 dB	×
Algorithm in [73]	pre-embedding	1.03%	59.63dB	×
Algorithm in [72]	pre-embedding	1.34%	36.97dB	√
Algorithm in [76]	pre-embedding	1.50%	29.03dB	×
Algorithm in [89]	post-embedding	2.44%	34.54dB	√
Algorithm in [90]	post-embedding	0.57%	37.05dB	√

4. Future popular video steganography

In this section, we introduce the future popular video steganography, including H.265 video steganography, robust video steganography and reversible video steganography.

4.1 H.265 Video steganography

H.265 is the latest video coding standard published by ITU-T/VCEG and ISO/IEC MPEG [94]. H.265's main achievement is its significant improvement in compression performance when compared to the previous state-of-the-art standard with at least 50% reduction in bitrate for producing video of similar perceptual quality [95], which is well adapted for high definition video applications and will become more popular video technologies. The significance of video steganography based on H.265 can be highlighted as follows: 1) with the growing popularity of HD (high definition) and the emergence of beyond-HD formats such as 8k×4k resolution, video steganography based on H.265 can effectively satisfy the needs for protection of the secret information related to the HD video content. 2) With the higher compression performance compared to H.264, the video steganography methods based on H.265 can obtain higher safe mechanism to conceal the secret message, better tradeoff between visual quality, embedding capacity and robustness, and make it more appropriate for HD network transmission.

The existing H.265 video data hiding schemes are studied by few scholars since H.265 is recently finalized. [24] employed the three-coefficients to solve the DST coefficient distortion drift problem for 4×4 luminance blocks in H.265. [25] furthered a group of decision conditions to increase the visual quality of embedded video, but the embedding capacity is reduced. [26] introduced a multivariate array to realize reversible steganography in 4×4 luminance DST blocks. However, each 4×4 luminance block can only be embedded in 1 bit of message, so the embedding capacity is limited. To solve the DCT coefficient distortion drift problem in H.265. [27] proposed a group of paired-coefficients for 8×8 luminance DCT blocks which had a similar effect to the paired-coefficients used in [16], but the visual quality is not ideal enough. [38] used the mapping between (4,3) code standard array decoding table and the intra prediction mode to reduce the impact of the prediction mode modulation, but the algorithm has a high complexity. [39] further utilized Local Binary Patterns (LBP) to scan high complexity texture as the embedding area. [40] developed the mapping relationship between the angle differences and secret message, which the embedding capacity is insufficient because the modulation range is too large. [41] optimized the mapping relationship with a Lagrange rate distortion model. Although the embedding capacity is slightly larger than [28], it is still limited. [56] created N-dimensional motion vector space with a mapping relationship and realized that a 2N+1-ary number can be embedded by modifying at most one element in a set of N motion vector components, which has high embedding efficiency. [96] proposed for H.265 video by using the coding block size feature in H.265 , the nonzero DCT coefficients are manipulated based on the transform block size in all slices and a data hiding technique is proposed to adaptively manipulate the prediction block size. These techniques have the potential to be further fine-tuned to handle. [97] modified the LSB of the selected QTCs and embedded one of the watermark bit (Mb) in each QTC. Consequently, further studies and investigations are required.

4.2 Robust video steganography

The robust video steganography (as shown in Fig.9) will become more popular because the security problem in information field is becoming more and more serious and the video has infinite sequences. And BCH [98-104], secret sharing [105-119] and Forbidden Zone [120-125] have been applied successfully to improve the robustness.

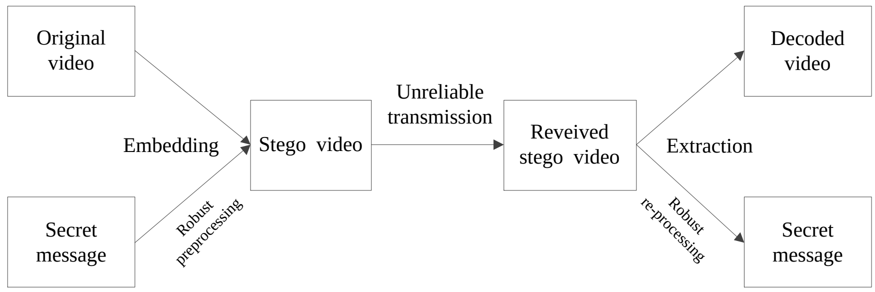


Fig.9 Robust video steganography

Bose, Chaudhuri, and Hocquenghem invented the BCH encoder. It is one of the most powerful random cyclic code methods, which can be used for detecting and correcting error bit. Binary BCH (n, k, t) codes can correct up to t errors, where n is the code-word length and k is the code dimension. The core generalized parity-check matrix *B* for BCH(*n*, *k*, *t*) can be represented as follows:

$$\mathrm{B}=\begin{bmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ 1 & \alpha^3 & \left(\alpha^3\right)^2 & \cdots & \left(\alpha^3\right)^{n-1} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & \alpha^{2t-1} & \left(\alpha^{2t-1}\right)^2 & \cdots & \left(\alpha^{2t-1}\right)^{n-1} \end{bmatrix} \tag{7}$$

Where α is the primitive element in Galois field $GF(2^m)$, *m* is the order of the Galois field $GF(2^m)$.

Let the single-bit error rate be *p*, then the error rate after BCH(*n*, *k*, *t*) encoding is as follows:

$$p_{BCH} \leq \sum_{i=t+1}^{n} \frac{i+t}{n} C_n^i p^i \ (1-p)^{n-i} \tag{8}$$

[99] proposed an efficient steganography method using BCH code. The embedding process is completed by changing various coefficients in order to make the syndrome values null. The method improves both capacity and computational time compared with other algorithms, which improves the system complexity from exponential to linear. In 2013, Liu et al. proposed a robust steganography scheme based on H.264 without intra-frame distortion drift. This process depends on the prediction of the intra-frame modes of neighboring blocks to avert the intra-frame distortion drift. To improve system efficiency and robustness, Liu et al. used BCH code before embedding message. Then, the encoded message is embedded into the 4x4 DCT block of quantized coefficients with a luminance component of the intra-frame [100]. In 2014, [101] proposed an adaptive steganography algorithm using a linear error correcting code and demonstrated that code is a better encoding algorithm than all other codes. In 2016, [103] improved [102] which proposed DCT-based robust video steganography

method using BCH error correcting codes, which converts the video into frames and divides each frame into Y, U, and V components. Prior to the embedding process, the secret message is encrypted and encoded by using BCH codes. And in 2015, a high payload video steganography algorithm in DWT domain is based on BCH codes.

The Shamir's (k, n)-threshold secret sharing (secret sharing) scheme provides an elegant construction of a perfect (t, n)-threshold scheme using a classical algorithm called Lagrange interpolation. Recently, the secret sharing has been used with video cryptography methods. In here, k $\leqslant$ n and the secret message is obtained when k secret shares are combined [105]. Some images and document data hiding techniques, etc based on secret sharing have been implemented in the literature [106-118]. [17] proposed a robust video steganography method using secret sharing resistance to the error frame. And [19-20] used secret sharing to improve the robustness of a reversible H.264 steganography. [119] presented a hierarchical frame work for video authentication based on cryptographic secret sharing that protects a video from spatial cropping and temporal jittering, yet is robust and resists frame dropping in the streaming video scenario.

Forbidden zone (FZ) is defined as the host signal range, where no alteration is allowed. Forbidden Zone Data Hiding (FZDH) makes use of FZ to adjust the robustness-invisibility trade-off. The embedder and decoder functions of FZDH are given in the paper [120]. Recently, Forbidden zone is used in video steganography[121-125]. [121] proposed a new video data hiding framework that makes use of erasure correction capability of repeat accumulate codes and superiority of FZDH. The proposed framework is tested by typical broadcast material against MPEG-2, H.264 compression, frame-rate conversion and frame manipulation attacks via frame synchronization markers. [123] implemented an advanced video data hiding method that performs erasure correction capability of repeat accumulate codes and superiority of forbidden zone data hiding. This method includes a temporal synchronization scheme in the sequence to resist insert attacks and frame drop. [125] made use of correction ability of duplication store codes and advantage of forbidden zone data hiding was used.

4.3 Reversible Video Steganography

In most cases, the video will be affected by some distortion after steganography and the processed video cannot be recovered completely. And, in some applications, such as medical diagnosis, military video, remote sensing video processing, legal certification and evidence, etc, they are critical to restore the original video [126]. Reversible steganography is a technique by which the original video can be recovered exactly, and it can be used in a variety of domains at present, as shown in Fig.10. Some reversible steganography techniques have been reported in some literatures, and most of the them are based on difference-expansion [128-134], histogram shifting [135-139], DCT coefficients [17-20,140-142,] and DWT, VQ, motion vector and so on [143-149], etc., to embed message.

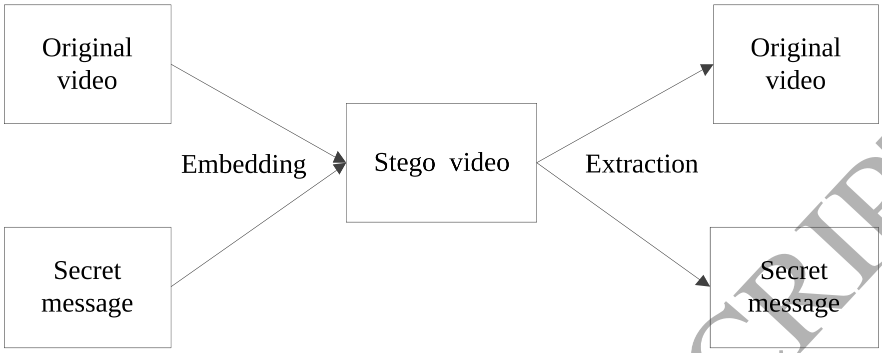


Fig.10 Reversible video steganography

The first reversible data hiding algorithm was the patent submitted by Bart [127]. After that, the reversible steganography algorithms were constantly emerging. In 2003, [133] proposed a difference-expansion image method without compressing the original medium，which achieved reversibility by the correlation of adjacent pixels. It was researched by many other researchers and had a profound impact on reversible steganography technology development [129-134]. [135] presented another representative reversible data hiding algorithm based on the histogram shifting, which utilized the zero or the minimum points of the histogram of an image and slightly modified the pixel brightness levels to embed message into the image. Afterwards, it has been improved by many researchers [136-139]. Currently, most of the existing reversible video steganography algorithms mainly embed the data into the DCT coefficients of I-frames [17-20, 26, 140-143,]. In [140], the authors presented a new reversible data hiding algorithm based on integer transform and adaptive embedding. [141-143] discussed a variety of robust data hiding algorithms in detail. There are many other methods that use other coefficients such as DWT, VQ, motion vector and so on [143-145]. In [145], the authors researched a novel high capacity reversible image data hiding scheme using a prediction technique which was effective for error resilience in H.264/AVC. Many other methods were presented in [146-151]. In previous work, most of the algorithms inevitably encountered distortion drift problem including intra and inter. And all the mentioned algorithms were only for 2D fields. [143] presented a reversible video steganography scheme for hiding secret message into the motion vector of each block in 3D MVC videos. [26] introduced a multivariate array to realize reversible steganography in 4×4 luminance DST blocks based on H.265.

4.4 Video steganography based on Artificial Intelligence

Video steganography is a multidisciplinary research area involving theory of communications, signal processing, multimedia coding, message theory, cryptography, etc. Artificial Intelligence (AI) including machine learning [152-155,174-182], pattern recognition [157-160,178-180], heuristic optimization [162-168] is one sub branch of computer science, which can be used to steganography technology and can achieve high visual quality, robustness, low cost, optimal and adaptive solutions. Recently, AI technology is rarely used in video steganography , though applied to various kinds of image steganography，including Particle Swarm Optimization [156, 161], Ant Colony Optimization [169-176], Neural Networks Support Vector Machine [177], Genetic Algorithms [181-190],and etc. In [186], the scheme based LSB has been used as a base technique for video steganography and GA has been used as an optimizer to modify embedded pixels coefficients, so that some target performance will be optimized. Fig. 11 shows how to use GA as an optimizer in [186]. Due to the generality of image steganography and pre-embedding video steganography, the AI technology applied to image steganography has great reference value for pre-embedding video steganography.

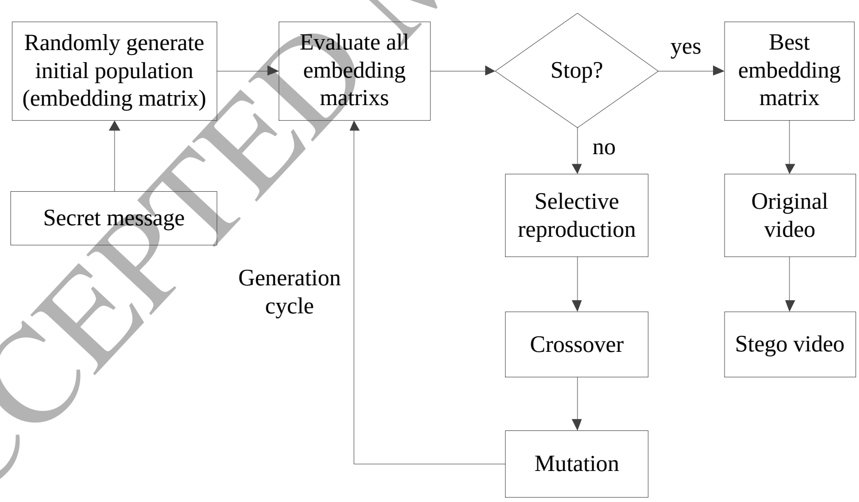


Fig.11 GA as an optimizer in [186]

5. Conclusion and challenges

In this paper, we have presented a systematic overview of the video steganography method, and the video steganography is divided into intra-embedding, pre-embedding and post-embedding according to the embedded position of secret information. The performance of video steganography and the future popular video steganography including H.265, robust, and reversible video steganography are also discussed. And the challenges on video steganography are shown as follows:

1) The video steganography method which can obtain a good trade-off between the performance of visual quality, high embedding capacity and strong robustness to resist a number of unexpected attacks is the first challenge.

2) The video steganography method which can be combined with other techniques such as artificial intelligence is the second challenge. Video steganography with artificial intelligence will enhance the visual quality and the secret protection of video steganography, which could use a portion of the video to embed data, for instance, embedding message could be embedded into the region of interest human behaviors, moving cars and so on.

3) The third challenge in video steganography is how to effectively combine the steganography with other protection technologies such as cryptography and error correcting codes, which can improve the security of the secret message and make the video steganography to be suitable for various unsafe application scenes.

6. Acknowledgment

This paper is sponsored by the National Natural Science Foundation of China (NSFC, Grant 61572447).

References

[1] "Video-HiDef Audio and Video". hidefnj.com. Archived from the original on 2017-05-14. Retrieved 2017-03-30.

[2] Mstafa R J, Elleithy K M, Abdelfattah E. Video steganography techniques: taxonomy, challenges, and future directions[C]//Systems, Applications and Technology Conference (LISAT), 2017 IEEE Long Island. IEEE, 2017: 1-6.

[3] Y. X. Liu, Z. T. Li, X. J. Ma and J. Liu. A robust without intra-frame distortion drift data hiding algorithm based on H.264/AVC[J]. Multimedia Tools and Applications. Springer, 2014, 72(1):613-636.

[4] Sadek M M, Khalifa A S, Mostafa M G M. Video steganography: a comprehensive review[J]. Multimedia tools and applications, 2015, 74(17): 7063-7094.

[5] D.S.Huang, “Radial basis probabilistic neural networks: Model and application,” International Journal of Pattern Recognition and Artificial Intelligence, 13(7), pp.1083-1101, 1999.

[6] D.S.Huang and S.D.Ma,“Linear and nonlinear feedforward neural network classifiers: A comprehensive understanding,”Journal of Intelligent Systems, vol.9, no.1, pp.1-38,1999.

[7] D.S.Huang, “A constructive approach for finding arbitrary roots of polynomials by neural networks,” IEEE Transactions on Neural Networks, vol.15, no.2, pp.477-491, 2004.

[8] D.S.Huang, Horace H.S.Ip, Law Ken C K and Zheru Chi, “Zeroing polynomials using modified constrained neural network approach,” IEEE Trans. On Neural Networks，vol.16, no.3, pp.721-732, 2005.

[9] D.S.Huang, W.B.Zhao,"Determining the centers of radial basis probabilistic neural networks by recursive orthogonal least square algorithms," Applied Mathematics and Computation, vol.162, no.1, pp.461-473, 2005.

[10] Mstafa R J, Elleithy K M. Compressed and raw video steganography techniques: a comprehensive survey and analysis[J]. Multimedia Tools and Applications, 2017, 76(20): 21749-21786.

[11] Shi Y Q, Li X, Zhang X, et al. Reversible data hiding: advances in the past two decades[J]. IEEE Access, 2016, 4: 3210-3237.

[12] Choudry, Kedar Nath, and Aakash Wanjari. "A Survey Paper on Video Steganography." International Journal of Computer Science and Information Technologies 6.3 (2015): 2335-2338.

[13] Noorkami M, Mersereau R M. A framework for robust watermarking of H. 264-encoded video with controllable detection performance[J]. IEEE Transactions on Information Forensics and Security, 2007, 2(1): 14-23.

[14] Gong X, Lu H M. Towards fast and robust watermarking scheme for H. 264 video[C]//Multimedia, 2008. ISM 2008. Tenth IEEE International Symposium on. IEEE, 2008: 649-653.

[15] X. J. Ma, Z. T. Li, J. L and W. D. Wang. Data Hiding in H.264/AVC Streams with Limited Intra-Frame Distortion Drift [C]. Computer network and Multimedia Technology, CNMT 2009.

[16] Ma X, Li Z, Tu H, et al. A data hiding algorithm for H. 264/AVC video streams without intra-frame distortion drift[J]. IEEE transactions on circuits and systems for video technology, 2010, 20(10): 1320-1330.

[17] Liu Y, Chen L, Hu M, et al. A reversible data hiding method for H. 264 with Shamir’s (t, n)-threshold secret sharing[J]. Neurocomputing, 2016, 188: 63-70.

[18] Y. X Liu, Z. T. Li, X. J. Ma. Reversible data hiding scheme based on H.264/AVC without distortion drift[J]. J. Syst. Software. 2012, 7(5):1059–1065.

[19] Y.X. Liu, S.M. Jia, M.S. Hu, et al. A robust reversible data hiding scheme for H.264 based on secret sharing[C]. ICIC2014, pp 553-559, 2014

[20] Y. X. Liu, L. M. Ju, M. S. Hu, X. J. Ma, H. G. Zhao. A robust reversible data hiding scheme for h.264 without distortion drift[J]. Neurocomputing, 151:1053-1062, 2015.

[21] Y.X. Liu, M.S. Hu, X.J. Ma, H.G. Zhao. A new robust data hiding method for H.264/AVC without intra-frame distortion drift [J]. Neurocomputing. 2015,1076-1085

[22] Y. X. Liu, L. M. Ju, M. S. Hu, et al. A new data hiding method for h.264 based on secret sharing [J]. Neurocomputing. 2016, 188:113-119

[23] Zhao J, Li Z T, Feng B. A novel two-dimensional histogram modification for reversible data embedding into stereo H. 264 video[J]. Multimedia Tools and Applications, 2016, 75(10): 5959-5980.

[24] Po-Chun Chang, Kuo-Liang Chung, Jiann-Jone Chen, Chien-Hsiung Lin. An Error Propagation Free Data Hiding Algorithm in H.265 Intra-Coded Frames [C]. Signal & Information Processing Association Summit & Conference, 2013: 1-9.

[25] Y X Liu, S Y Liu, H G Zhao, S Liu, C Feng. A Data Hiding Method for H.265 Without Intra-frame Distortion Drift[C]. International Conference on Intelligent Computing, 2017, 2017(1):642-650

[26] S Liu, Y X Liu, C Feng, H G Zhao. A Reversible Data Hiding Method Based on H.265 Without Distortion Drift[C]. International Conference on Intelligent Computing, 2017, 2017(1):613-624

[27] Po-Chun Chang, Kuo-Liang Chung, Jiann-Jone Chen, Chien-Hsiung Lin ,etc. A DCT/DST-based error propagation-free data hiding algorithm for H.265 intra-coded frames [J]. Journal of Visual Communication & Image Representation. 2013, 25(2):239–253

[28] HU, Yang; ZHANG, Chun-tian; SU, Yu-ting. Information hiding for H.264/AVC. Acta Electronica Sinica, 2008, 36.4: 690.

[29] Wang, R., Zhu, H., & Xu, D. Information hiding algorithm for H.264/AVC based on encoding mode. Opto-Electronic Engineering, 2010, 37(5), 144-150.

[30] Xu, D. W., Wang, R. D., & Wang, J. C. Prediction mode modulated data-hiding algorithm for H.264/AVC. Journal of Real-Time Image Processing, 2014, 7(4), 205-214.

[31] Yang, G. B., Li, J. J., He, Y. L., & Kang, Z. W. An information hiding algorithm based on intra-prediction modes and matrix coding for H.264/AVC video stream. AEU-International Journal of Electronics and Communications, 2011, 65(4), 331-337.

[32] Yin, Q., Wang, H., & Zhao, Y. An information hiding algorithm based on intra-prediction modes for H.264 video stream. Journal of Optoelectronics. Laser, 2012, 23(11), 2194-2199.

[33] Bouchama, S., Hamami, L., Aliane, H. H.264/AVC data hiding based on intra prediction modes for real-time applications. Lecture Notes in Engineering and Computer Science, 2012, vol. 1, 655-658.

[34] Zhang, L., Zhao, X. An adaptive video steganography based on intra-prediction mode and cost assignment. IWDW 2016. LNCS, 2016, vol. 10082, pp. 518–532.

[35] Wang Y, Cao Y, Zhao X, et al. A prediction mode-based information hiding approach for H.264/AVC videos minimizing the impacts on rate-distortion optimization. International Workshop on Digital Watermarking. Springer, Cham, 2017: 163-176.

[36] Zhao, Y., Zhang, H., Cao, Y., Wang, P., Zhao, X. Video steganalysis based on intra prediction mode calibration. 2015 International Workshop on Digital-forensics and Watermarking, 2015, 119-133.

[37] NIE, Qiankai, et al. Defining Embedding Distortion for Intra Prediction Mode-based Video Steganography. Computers, Materials & Continua, 2018, 55.1: 59-59.

[38] Wang, J., R., Wang, W., Li, Xu, D., & Huang. M. An Information hiding algorithm for H.265 based on intra prediction mode and block code. Sensors & Transducers, 2014, 177(8), 230-237.

[39] Wang, J., Wang, R., Xu, D., Li, W., Yan, D. An information hiding algorithm for H.265 based on intra prediction modes. J. Optoelectron. Laser, 2014, 25(8), 1578–1585

[40] Wang, J., Wang, R, Dawen, X., Li, W., Yan, D. An information hiding algorithm for H.265 based on angle differences of intra prediction mode. J. Softw, 2015, 10(2), 213–221.

[41] Sheng Q, Wang R, Pei A, et al. An Information Hiding Algorithm for H.265 Based on Differences of Intra Prediction Modes. International Conference on Cloud Computing and Security, Springer, Cham, 2016: 63-74.

[42] Jordan F, Kutter M, Ebrahimi T, Jordan F. Proposal of a watermarking technique for hiding/retrieving data in compressed and decompressed video. Technical Report M2281, ISO/IEC document, JTCI/SC29/WG11, 1997.

[43] Xu C, Ping X, Zhang T. Steganography in compressed video stream. In Proc. ICICIC'06, 2006, 269–272.

[44] Fang DY, Chang LW. Data hiding for digital video with phase of motion vector. In: Proceedings of the international symposium on circuit and systems, 2006, pp 1422–1425

[45] X. He, Z. Luo. A novel steganographic algorithm based on the motion vector phase. In Proc. Int. Conf. Comp. Sc. and Software Eng., 2008, pp. 822–825.

[46] Aly H. Data hiding in motion vectors of compressed video based on their associated prediction error. IEEE Trans Inf Forensic Secur, 2011, 6(1):14–18.

[47] Guo Y, Pan F. Message hiding for H.264 in video stream switching application.In Proceedings of the 2010 IEEE international conference on message theory and message security, 2010, pp 419–421.

[48] Hao B, Zhao L, Zhong W. A novel steganography algorithm based on motion vector and matrix encoding. In Proc. ICCSN'11, 2011, pp. 406–409.

[49] Cao Y, Zhao X, Feng D, Sheng R. Video steganography with perturbed motion estimation. Proc IH'11 Lect Notes Comput Sci, 2011, 6958:193–207.

[50] Fridrich J, Goljan M, Lison•ek P, Soukal D. Writing on wet paper. IEEE Trans Signal Process, 2005, 53(10): 3923–3935.

[51] Su Y, Zhang C, Zhang C. Avideo steganalytic algorithm against motion-vector-based steganography. Signal Process, 2011, 91(8):1901–1909.

[52] Zhu HL, Wang RD, Xu DW (2010) Message hiding algorithm for H.264 based on the motion estimation of quarter-pixel. In: Proceedings of the 2nd international conference future computer communication, pp 423–427

[53] Swaraja K, Latha YM, Reddy VSK, Paramkusam AV (2011) Video watermarking based on motion vectors of H.264. In: Proceedings of the 2011 annual IEEE india conference, pp 1–4

[54] Yao YZ, Zhang WM, Yu NH, Zhao XF.Defining embedding distortion for motion vector-based video steganography. Multimed Tools Appl, 2015, 74(24):11163–11186.

[55] Filler T, Judas J, Fridrich J. Minimizing additive distortion in steganography using syndrome-trellis codes. IEEE Trans Inf Forensic Secur, 2011, 6(3):920–935

[56] Yang J, Li S. An efficient message hiding method based on motion vector space encoding for H.265 . Multimedia Tools and Applications, 2017: 1-23.

[57] Niu K, Yang X, Zhang Y.A novel video reversible data hiding algorithm using motion vector for H. 264/AVC. Tsinghua Science and Technology, 2017, 22(5): 489-498.

[58] Cao Y, Zhao X, Feng D. Video steganalysis exploiting motion vector reversion-based features. IEEE Signal Process Lett, 2012, 19(1):35–38.

[60] Fridrich J. Feature-based steganalysis for jpeg images and its implications for future design of steganographic schemes. Proc. IH'04 Lect Notes Comput Sci 3200/2005, 2004, 67–81.

[61] Wang K, Zhao H, Wang H. Video steganalysis against motion vector-based steganography by adding or subtracting one motion vector value. IEEE Trans Inf Forensic Secur, 2014, 9(5):741–751.

[62] Ren Y, Zhai L, Wang L, Zhu T. Video steganalysis based on subtractive probability of optimal matching feature. In Proc ACM IH and MMSec'14, 2014, 83–90.

[62] Zhai L, Wang L, Ren Y. Combined and Calibrated Features for Steganalysis of Motion Vector-Based Steganography in H. 264/AVC.Proceedings of the 5th ACM Workshop on Message Hiding and Multimedia Security. ACM, 2017: 135-146.

[63]Zhang H, Cao Y, Zhao X. A steganalytic approach to detect motion vector modification using near-perfect estimation for local optimality[J]. IEEE Transactions on Message Forensics and Security, 2017, 12(2): 465-478.

[64]Wang P, Cao Y, Zhao X. Segmentation Based Video Steganalysis to Detect Motion Vector Modification[J]. Security and Communication Networks, 2017, 2017:1-12.

[65] Zhang H, Cao Y, Zhao XF.Motion vector-based video steganography with preserved local optimality. Multimed Tools Appl, 2016, 75(21):13503–13519.

[66] Ramalingam M. Stego machine–video steganography using modified LSB algorithm[J]. World

Academy of Science, Engineering and Technology, 2011, 74: 502-505.

[67] Dasgupta K, Mandal J K, Dutta P. Hash based least significant bit technique for video steganography (HLSB)[J]. International Journal of Security, Privacy and Trust Management (IJSPTM), 2012, 1(2): 1-11.

[68] Kaur M, Kaur A. Improved Security Mechanism of Text in Video using Steganographic Technique[J].International Journal of Advance Research in Computer Science and Management Studies, 2014, 2(10).

[69] Nishi Khan K, Gorde S. Video Steganography by Using Statistical Key Frame Extraction Method and LSB Technique[J].International Journal of Innovative Research in Science, Engineering and Technology, 2015, 4(10).

[70] Cetin O, Ozcerit A T. A new steganography algorithm based on color histograms for data embedding into raw video streams[J]. computers & security, 2009, 28(7): 670-682.

[71] Cetin O, Akar F, Ozcerit A T, et al. A blind steganography method based on histograms on video files[J]. The Imaging Science Journal, 2012, 60(2): 75-82.

[72] Alavianmehr M A, Rezaei M, Helfroush M S, et al. A lossless data hiding scheme on video raw data robust against H. 264/AVC compression[C]//Computer and Knowledge Engineering (ICCKE), 2012 2nd International eConference on. IEEE, 2012: 194-198.

[73] Cheddad A, Condell J, Curran K, et al. Skin tone based steganography in video files exploiting the YCbCr colour space[C]//Multimedia and Expo, 2008 IEEE International Conference on. IEEE, 2008: 905-908.

[74] Khupse S, Patil N N.An adaptive steganography technique for videos using Steganoflage[C]//Issues and Challenges in Intelligent Computing Techniques (ICICT), 2014 International Conference on. IEEE, 2014: 811-815.

[75] Mstafa R J, Elleithy K M. A video steganography algorithm based on Kanade-Lucas-Tomasi tracking algorithm and error correcting codes[J]. Multimedia Tools and Applications, 2016, 75(17): 10311-10333.

[76] Hu S D. A novel video steganography based on non-uniform rectangular partition[C]//The 14th IEEE International Conference on Computational Science and Engineering. IEEE, 2011: 57-61.

[77] Ramalingam M, Isa N A M. Fast retrieval of hidden message using enhanced hidden Markov model in video steganography[J]. Applied Soft Computing, 2015, 34: 744-757.

[78] Patel K, Rora K K, Singh K, et al. Lazy wavelet transform based steganography in video[C]//Communication Systems and Network Technologies (CSNT), 2013 International Conference on. IEEE, 2013: 497-500.

[79] Mstafa R J, Elleithy K M. A novel video steganography algorithm in the wavelet domain based on the KLT tracking algorithm and BCH codes[C]//Systems, Applications and Technology Conference (LISAT), 2015 IEEE Long Island. IEEE, 2015: 1-7.

[80] Sadek M M, Khalifa A S, Mostafa M G M. Robust video steganography algorithm using adaptive skin-tone detection[J]. Multimedia Tools and Applications, 2017, 76(2): 3065-3085.

[81] Mstafa R J, Elleithy K M. A novel video steganography algorithm in DCT domain based on hamming and BCH codes[C]//Sarnoff Symposium, 2016 IEEE 37th. IEEE, 2016: 208-213.

[82] Ramalingam M, Isa N A M. A data-hiding technique using scene-change detection for video steganography[J]. Computers & Electrical Engineering, 2016, 54: 423-434.

[83] Mstafa R J, Elleithy K M, Abdelfattah E. A robust and secure video steganography method in DWT-DCT domains based on multiple object tracking and ecc[J]. IEEE Access, 2017, 5: 5354-5365.

[84] Zhang Y, Zhang M, Wang X A, et al. A Novel Video Steganography Algorithm Based on Trailing Coecients for H. 264/AVC[J]. Informatica, 2015, 40(1).

[85] Shukur W A, Abdullah W N, Qurban L K. Information Hiding In Digital Video Using DCT, DWT and CvT[C]//Journal of Physics: Conference Series. IOP Publishing, 2018, 1003(1): 012035.

[86] Shahid Z, Chaumont M, Puech W. Fast protection of H.264/AVC by selective encryption[C]//Proceedings Of The Singaporean-French Ipal Symposium 2009: SinFra'09. 2009: 11-21.

[87] Shahid Z, Chaumont M, Puech W. Fast protection of H. 264/AVC by selective encryption of CAVLC and CABAC for I and P frames[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2011, 21(5): 565-576.

[88] Wang Y, O'Neill M, Kurugollu F. A tunable encryption scheme and analysis of fast selective encryption for CAVLC and CABAC in H. 264/AVC[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2013, 23(9): 1476-1490.

[89] Ke N Weidong Z (2013) Avideo steganography scheme based on H. 264 bitstreams replaced In: 4th IEEE International Conference on Software Engineering and Service Science (ICSESS), pp 447–450.

[90] Wang R, HU L Xu D (2011) A watermarking algorithm based on the CABAC entropy coding for H.264/AVC. J Comput Inform Syst 7(6):2132–2141.

[91] Xu D, Wang R. Context adaptive binary arithmetic coding-based data hiding in partially encrypted H. 264/AVC videos[J]. Journal of Electronic Imaging, 2015, 24(3): 033028.

[92] Xu D, Wang R, Zhu Y. Tunable data hiding in partially encrypted H. 264/AVC videos[J]. Journal of Visual Communication and Image Representation, 2017, 45: 34-45.

[93] Marpe D, Schwarz H, Wiegand T. Context-based adaptive binary arithmetic coding in the H. 264/AVC video compression standard[J]. IEEE Transactions on circuits and systems for video technology, 2003, 13(7): 620-636.

[94] G. J. Sullivan, J.-R. Ohm, W.-J Han, and T. Wiegand, “Overview of the High Efficiency Video Coding (H.265) standard,” IEEE Trans. Circuits Syst. Video

[95] R. J. Mstafa, K. M. Elleithy, "A highly secure video steganography using Hamming code (7 4)", Systems Applications and Technology Conference (LISAT) 2014 IEEE Long Island, pp. 1-6, 2014

[96] Yiqi Tew, KokSheik Wong: Information hiding in H.265 standard using adaptive coding block size decision. ICIP 2014: 5502-5506

[97] Swati S, Hayat K, Shahid Z. A watermarking scheme for high efficiency video coding (H.265)[J]. PloS one, 2014, 9(8): e105613.

[98] R. Zhang, V. Sachnev, and H. Kim, "Fast BCH Syndrome Coding for-Steganography," in Information Hiding. vol. 5806, S. Katzenbeisser and A.-R. Sadeghi, Eds., ed: Springer Berlin Heidelberg, 2009, pp. 48-58.

[99] R. Zhang, V. Sachnev, M. B. Botnan, H. J. Kim, and J. Heo, "An efficient embedder for BCH coding for Steganography," Information Theory, IEEE Transac-tions on, vol. 58, pp. 7272-7279, 2012.

[100] Y. Liu, Z. Li, X. Ma, and J. Liu, "A Robust Data Hiding Algorithm for H. 264/AVC Video Streams," Journal of Systems and Software, 2013.

[101] I. Diop, S. M. Farss, K. Tall, P. A. Fall, M. L. Diouf, and A. K. Di-op,"Adaptive steganography scheme based on LDPC codes," in 2014 16th International Conference on Advanced Communication Technology (ICACT), 2014, pp. 162-166.

[102] Mstafa R J, Elleithy K M. A high payload video steganography algorithm in DWT domain based

on BCH codes (15, 11)[C]// Wireless Telecommunications Symposium. IEEE, 2015:1-8.

[103] Mstafa R J, Elleithy K M. A highly secure video steganography using Hamming code (7, 4)[C]// Systems, Applications and Technology Conference. IEEE, 2014:1-6.

[104] Mstafa R J, Elleithy K M. A DCT-based robust video steganographic method using BCH error correcting codes[C]// Long Island Systems, Applications and Technology Conference. IEEE, 2016:1-6.

[105] Shamir, A.: How to share a secret. Commun. ACM 22(11), 612–613 (1979)

[106] Naor, M.; Shamir, A.: Visual cryptography. In: De Santis, A.(ed.) Advances in Cryptology—EUROCRYPT'94. Lecture Notes in Computer Science, vol. 950, pp. 1–12. Springer, Berlin, Heidelberg(1994)

[107] Sencar, H.T.; Ramkumar, M.; Akansu, A.N.: Data Hiding Fundamentals and Applications, Content Security in Digital Media. Elsevier Academic Press, Boston (2004)

[108] Miller, A.: Least Significant Bit Embeddings: Implementation And Detection (2012)

[109] Schyndel, R.G.V.; Tirkel, A.Z.; Osborne, C.F.: A digital watermark. In: Proceedings of IEEE International Conference of Image Processing 2, pp. 86–90, Austin, Texas (1994)

[110] Sun, G.; Yu, Y.: DWT based watermarking algorithm of color images. In: Second IEEE Conference on Industrial Electronics and Application, pp. 1823–1826 (2007)

[111] Lee, C.-W.; Tsai, W.-H.: A secret-sharing-based method for authentication of grayscale docu-ment images via the use of the PNG image with a data repair capability.IEEE Trans. Image Process. 21(1), 207–218 (2011)

[112] Lee, C.-W.; Tsai, W.-H.: A data hiding method based on information sharing via PNG images for applications of color image authentication and metadata embedding. Signal Process. 93(7), 2010–2025 (2013)

[113] Gurung, S.; Chakravorty, M.; Agarwal, A.; Ghose, M.K.: Multiple information hiding using circular random grids. Proc. Comput. Sci. 48, 65–72 (2015)

[114] Tu, S.-F.; Hsu, C.-S.: Protecting secret documents via a sharing and hiding scheme. Inf. Sci. 279(20), 52–59 (2014)

[115] Yuan, H.D.: Secret sharing with multi-cover adaptive steganography. Inf. Sci. 254, 197–212 (2014)

[116] Tuncer, T.; Avci, E.: A reversible data hiding algorithm based on probabilistic DNA-XOR secret sharing scheme for color images. Displays 41, 1–8 (2016)

[117] Sweldens,W.: The lifting scheme: a construction of second generation wavelets. SIAM J. Math. Anal. 29(2), 511–546 (1998)

[118] Avci E, Tuncer T, Avci D. A Novel Reversible Data Hiding Algorithm Based on Probabilistic XOR Secret Sharing in Wavelet Transform Domain[J]. Arabi-an Journal for Science & Engineering, 2016, 41(8):3153-3161.

[119] Atrey P K, Yan W Q, Chang E C, et al. A Hierarchical Signature Scheme for Robust Video Authentication using Secret Sharing[C]// Multimedia Model-ling Conference, 2004.Proceedings. International. IEEE, 2004:330.

[120] Esen E, Alatan A A. Forbidden Zone Data Hiding[J]. 2006:1393-1396.

[121] Ersin Esen and A. Aydin Alatan..Robust Video Data Hiding Using Forbid-den Zone Data Hiding and Selective Embedding. IEEE Transactions on Cir-cuits and Systems for Video Technology, 2011, 21(8): 1130-1138

[122] Radhika, V., & Krishnaiah, D. R. V.. An approach towards efficient video data hiding using prohibited zone. Ijitr. 2013

[123] Adepu M S, Ashok M P, Rao D C V G. A Security Mechanism for Video Data Hiding[J]. International Journal of Computer Trends & Technology, 2013, 4(8):2951-2955.

[124] Esen E, Alatan A A. Robust Video Data Hiding Using Forbidden Zone Data Hiding and Selective Embedding[M]. IEEE Press, 2011.

[125] Kalyan Chakravarthy P, Monica C M S, Gideon J K, et al. A Three Way Re-versible Encipherment Mechanisms for Robust Video Data Hiding Using Se-lective Embedding and Forbidden Zone Data Hiding[J]. International Journal of Computer Science & Information Technolo, 2014.

[126] Celik MU, Sharma G, Tekalp AM, Saber E (2002) Reversible data hiding. Proc IEEE Int Conf Image Process 2:157–160

[127] Barton JM,Method and apparatus for embedding authentication information within digital data. 1997, US Patent 6,115,818.

[128] Tian J (2003) Reversible data embedding using a difference expansion. IEEE Trans Circuits Syst Video Technol 13(8):890–896

[129] Alattar AM (2004) Reversible watermark using the difference expansion of a generalized integer transform [J]. IEEE Transactions on Image Processing 13(8):1147–115

[130] Chang CC, Lu TC (2006) A difference expansion oriented data hiding scheme for restoring the original host images [J]. The Journal of Systems & Software 79(12):1754–1766

[131] Hong W, Chen TS, Chang YP, Shiu CW (2010) A high capacity reversible data hiding scheme using orthogonal projection and prediction error modification. Signal Process 90(11):2911–2922

[132] Hsien-Wen T, Chi-Chen C (2008) An extended difference expansion algorithm for reversible Watermarking[J]. Image and Vision Computing 26(8):1148–1153

[133] Hu Y, Lee H-K, Li J (2009) DE-based reversible data hiding with improved overflow location map. IEEE Trans Circuits Syst Video Technol 19(2):250–260

[134] Thodi D M, Rodriguez J J. Reversible watermarking by Prediction-error expansion[C], IEEE Southwest Symposium on Image Analysis and Interpretation, Arizona, USA, 2004:21-25

[135] Ni Z et al (2006) Reversible Data Hiding. IEEE Trans Circuits Syst Video Technol 16(3):354–362

[136] Chang CC, Tai WL, Lin CC (2006) A reversible data hiding scheme based on side-match vector quantization. IEEE Trans Circuits Syst Video Technol 16(10):1301–1308

[137] Hwang J, Kim JW, Choi JU (2006) A reversible watermarking based on histogram shifting, Int. Workshop on Digital Watermarking, Lecture Notes in Computer Science 4283:348–361

[138]Thodi DM, Rodriguez JJ (2007) Expansion embedding techniques for reversible watermarking [J]. IEEE Tran On Image Processing 16(3):721–730

[139] Tsai P, Hu YC, Yeh HL (2009) Reversible image hiding scheme using predictive coding and histogram shifting. Signal Process 89:1129–1143

[140]Qin C, Chang CC, Huang YH, Liao LT (2012) An Inpainting-Assisted Reversible Steganographic Scheme Using Histogram Shifting Mechanism. IEEE Transactions on Circuits and Systems for Video Technology, (99): 1–11

[141] Kim S, Hong Y, Won C (2007) Data hiding on H.264/AVC compressed video. Image Anal Recog 4633(2007):698–707

[142]Noorkami M, Mersereau RM (2007) A framework for robust watermarking of H.264-encoded video with controllable detection performance. IEEE Trans Inform Forensics Security 2(1):14–23

[143] Song G, Li Z, Zhao J, et al. A reversible video steganography algorithm for MVC based on motion vector[J]. Multimedia Tools & Applications, 2015, 74(11):3759-3782.

[144] Lie WN, Lin CI, Tsai DC, Lin GS (2005) Error resilient coding based on reversible data embedding technique for H.264/AVC video. Proc. IEEE Int. Conf. Multimedia and Expo 1174–1177
[145] Fallahpour M, Megías D (2009) Reversible Data Hiding Based on H.264/AVC Intra Prediction. Lecture Notes in Computer Science, no.5450. Springer, Berlin, pp 52–60
[146] Cao Y, Zhao X, Feng D (2012) Video steganalysis exploiting motion vector reversion-based features. IEEE Signal Process Lett 19(1):35–38
[147] Fallahpour M, Megias D, Ghanbari M (2011) Reversible and high-capacity data hiding in medical images. IET Image Processing 5(2):190–197
[148] Profrock D, Richter H, Schlauweg M, Muller E (2005) H.264-AVC video authentication using skipped macroblocks for an erasable watermark. Proc SPIE Visual Commun Image Process 5960: 1480–1489
[149] Yang CY, Lin CH, Hu WC (2011) Reversible data hiding by adaptive IWT-coefficient adjustment. Journal of Information Hiding and Multimedia Signal Processing 2(1):24–32
[150] Ho YS, Oh KJ. Overview of multi-view video coding. Proc. 14th Int. Workshop Syst. Signals Image Process., 6th EURASIP Conf. Focused Speech Image Process., Multimedia Commun. Services, pp.5–12 2007.
[151] Merkle P, Smolic A, Mueller K, Wiegand T (2007) Efficient prediction structures for multiview video coding. IEEE Trans Circuits Syst Video Technol 17(11):1461–1473
[152] Fei Han, D.S.Huang,"Improved extreme learning machine for function approximation by encoding a priori information," Neurocomputing, vol.69, nos.16-18, pp.2369-2373, 2006.
[153] Fei Han, D.S.Huang,"A new constrained learning algorithm for function approximation by encoding a priori information into feedforward neural networks," Neural Computing and Applications, vol.17, nos.5-6, pp.433-439, 2008.
[154] Fei Han, Qing-Hua Ling, and D.S.Huang,"Modified constrained learning algorithms incorporating additional functional constraints into neural networks," Information Sciences, vol.178, no.3, pp.907-919, 2008.
[155] Zhong-Qiu Zhao, D.S.Huang,"A mended hybrid learning algorithm for radial basis function neural networks to improve generalization capability," Applied Mathematical Modelling, vol.31, no.7, pp. pp.1271-1281, 2007.
[156] Naheed T, Usman I, Khan T M, et al. Intelligent reversible watermarking technique in medical images using GA and PSO[J]. Optik-International Journal for Light and Electron Optics, 2014, 125(11): 2515-2525.
[157] D.S.Huang,Systematic Theory of Neural Networks for Pattern Recognition, Publishing House of Electronic Industry of China, May 1996.
[158] Ji-Xiang Du, D.S.Huang, Xiao-Feng Wang, Xiao Gu, "Shape recognition based on neural networks trained by differential evolution algorithm," Neurocomputing, vol.70, nos.4-6, pp. 896-903, 2007.
[159] Li Shang, D.S.Huang, Ji-Xiang Du, and Chun-Hou Zheng, " Palmprint recognition using FastICA algorithm and radial basis probabilistic neural network," Neurocomputing, vol.69, nos.13-15, pp. 1782-1786, 2006.
[160] Zhong-Qiu Zhao, D.S.Huang,"Palmprint recognition with 2DPCA+PCA based on modular neural networks," Neurocomputing, vol.71, nos.1-3, pp. 448-454, 2007.
[161] Divya E, Kumar P R. Steganographic data hiding using modified APSO[J]. International Journal of Intelligent systems and applications, 2016, 8(7): 37.

[162] D.S.Huang, Ji-Xiang Du, "A constructive hybrid structure optimization methodology for radial basis probabilistic neural networks," IEEE Transactions on Neural Networks, vol. 19, no.12, pp 2099-2115, 2008.

[163] Khamrui A, Mandal J K. A genetic algorithm based steganography using discrete cosine transformation (GASDCT)[J]. Procedia Technology, 2013, 10: 105-111.

[164] Ji-Xiang Du, D.S.Huang, Guo-Jun Zhang and Zeng-Fu Wang,"A novel full structure optimization algorithm for radial basis probabilistic neural networks," Neurocomputing, vol.70, nos.1-3, pp. 592-596, 2006.

[165] W.B.Zhao, D.S.Huang, Ji-Yan Du and Li-Ming Wang, "Genetic optimization of radial basis probabilistic neural networks," International Journal of Pattern Recognition and Artificial Intelligence, vol. 18, no. 8, pp. 1473-1500, 2004.

[166] Zhan-Li Sun, D.S.Huang, and Chun-Hou Zheng, Li Shang, "Optimal selection of time lags for temporal blind source separation based on genetic algorithm," Neurocomputing, vol.69, nos.7-9, pp.884–887, 2006.

[167] Fei Han, Qing-Hua Ling, and D.S.Huang,"An improved approximation approach incorporating particle swarm optimization and a priori information into neural networks," Neural Computing & Applications, vol. 19, no.2, pp. 255-261, 2010.

[168] C.C. Chang and I. C. Lin, A perceptually tuned watermarking scheme for digital images using supprot vector machines, Intelligent Watermarking Techniques, (World Scientific, Singapore 2004)429-457.

[169] Douiri S M, Elbernoussi S. An ant colony optimisation for data hiding in greyscale images[J]. International Journal of Operational Research, 2017, 29(1): 101-114.

[170] Zhan-Li Sun, D.S.Huang, and Yiu-Ming Cheung, "Extracting nonlinear features for multispectral images by FCMC and KPCA," Digital Signal Processing, vol.15, no.4, 331-346, 2005.

[171] Zhan-Li Sun, D.S.Huang, Yiu-Ming Cheung, Jiming Liu and Guang-Bin Huang, "Using FCMC, FVS and PCA techniques for feature extraction of multispectral images," IEEE Geoscience and Remote Sensing Letters, vol.2, no.2, pp.108-112, 2005.

[172] Khan S, Bianchi T. Ant Colony Optimization (ACO) based Data Hiding in Image Complex Region[J]. International Journal of Electrical and Computer Engineering (IJECE), 2018, 8(1): 379-389.

[173] Chun-Hou Zheng, D.S.Huang, and Li Shang, "Feature selection in independent component subspace for microarray data classification," Neurocomputing, vol.69, nos.16-18, pp.2407-2410, 2006.

[174] Alam S, Ahmad T, Doja M N. A Chaotic Steganography Method Using Ant Colony Optimization[M]//Intelligent Engineering Informatics. Springer, Singapore, 2018: 431-439.

[175] Bo Li, D.S.Huang, Chao Wang and Kun-Hong Liu, "Feature extraction using constrained maximum variance mapping," Pattern Recognition, vol.41, no.11, pp. 3287-3294, 2008.

[176] Xiao-Feng Wang, D.S.Huang, "A novel density-based clustering framework by using level set method," IEEE Transactions on Knowledge and Data Engineering, vol. 21, no.11, pp 1515-1531, 2009.

[177] C.C. Chang and I. C. Lin, Robust image watermarking system using neural network, Intelligent Watermarking Techniques(World Scientific, Singapore 2004) 395-427.

[178] Bo Li, Chao Wang and D.S.Huang, "Supervised feature extraction based on orthogonal discriminant projection," Neurocomputing, vol. 73, nos.1-3, pp 191-196, 2009.

[179] Yang Zhao, and D.S.Huang, "Completed local binary count for rotation invariant texture classification," IEEE Trans. on Image Processing, vol.21, no.10, pp. 4492 - 4497, 2012.

[180] Can-Yi Lu, and D.S.Huang, "Optimized projections for sparse representation based

classification,” Neurocomputing, vol.113, pp.213-219, 2013.
[181] Chatterjee A, Barik N. A New Data Hiding Scheme Combining Genetic Algorithm and Artificial Neural Network[M]//Handbook of Research on Modeling, Analysis, and Application of Nature-Inspired Metaheuristic Algorithms. IGI Global, 2018: 94-103.
[182] D.S. Huang, The Study of Data Mining Methods for Gene Expression Profiles, Science Press of China, March 2009.
[183] Bo Li, and D.S.Huang, “Locally linear discriminant embedding: An efficient method for face recognition,” Pattern Recognition, vol.41, no.12, pp. 3813-3821, 2008.
[184] Siar F, Alirezazadeh S, Jalali F. A novel steganography approach based on ant colony optimization[C]//Fuzzy and Intelligent Systems (CFIS), 2018 6th Iranian Joint Congress on. IEEE, 2018: 215-219.
[185] Chun-Hou Zheng, D.S.Huang, Zhan-Li Sun, Michael R. Lyu, and Tat-Ming Lok, "Nonnegative independent component analysis based on minimizing mutual information technique," Neurocomputing, vol.69, nos.7-9, pp.878－883, 2006.
[186] Dasgupta K, Mondal J K, Dutta P. Optimized video steganography using genetic algorithm (GA)[J]. Procedia Technology, 2013, 10: 131-137.
[187] Jian-Xun Mi, D.S.Huang, Bing Wang, Xingjie Zhu, “The nearest-farthest subspace classification for face recognition,” Neurocomputing, vol.113, pp.241-250, 2013.
[188] Maity S P, Kundu M K. Genetic algorithms for optimality of data hiding in digital images[J]. Soft computing, 2009, 13(4): 361-373.
[189] Doğan Ş. A new data hiding method based on chaos embedded genetic algorithm for color image[J]. Artificial Intelligence Review, 2016, 46(1): 129-143.
[190] Wang J, Ni J, Zhang X, et al. Rate and Distortion Optimization for Reversible Data Hiding Using Multiple Histogram Shifting[J]. IEEE Trans. Cybernetics, 2017, 47(2): 315-326.

YunXia Liu was born in Zhoukou, China in 1972, and received her B.E. degree from Henan Normal University, Xinxiang, China, 1996, and PhD degree from Huazhong University of Science and Technology, Wuhan, China, 2013. She is a professor in the college of information science and technology at Zhengzhou Normal University. Her research interests include: cryptography, network security and multimedia security.

Shuyang Liu was born in Zhoukou, China in 1998. He is a college student in the school of mathematics and statistics at Lanzhou University. His research interests include: mathematical modelling, scientific computing and network security.

YongHao Wang was born in JiangSu, China in 1977, and received her B.E. degree from Nanjing University of Science and Technology, China, 1999, and MSc degree from University of Central England in Birmingham, UK 2002. He is a Senior Lecturer in the DMT inLab of School of Computing and Digital Technology at Birmingham City University. His research interests include: digital signal processing, multimedia network distribution and information security.

Hongguo Zhao was born in Shanxi, China in 1990, and received his master degree from Huazhong University of Science and Technology, Wuhan, China, 2014. He is a Lecturer in the college of information science and technology at Zhengzhou Normal University. His research interest is information hiding and etwork security.

Si Liu was born in Xinyang, China in 1985, and received his master degree from Zhengzhou University of Light Industry, Zhengzhou, China, 2011. He is a Lecturer in the college of information science and technology at Zhengzhou Normal University. His research interest is information hiding and artificial Intelligence.

ACCEPTED MANUSCRIPT