# Video Steganography Techniques: Taxonomy, Challenges, and Future Directions

Ramadhan J. Mstafa and Khaled M. Elleithy
Department of Computer Science and Engineering
University of Bridgeport
Bridgeport, CT 06604, USA
*rmstafa@my.bridgeport.edu , elleithy@bridgeport.edu*

Eman Abdelfattah
School of Computing
Sacred Heart University
Fairfield, CT 06825, USA
*abdelfattahe@sacredheart.edu*

***Abstract*—Nowadays, video steganography has become important in many security applications. The performance of any steganographic method ultimately relies on the imperceptibility, hiding capacity, and robustness. In the past decade, many video steganography methods have been proposed; however, the literature lacks of sufficient survey articles that discuss all techniques. This paper presents a comprehensive study and analysis of numerous cutting edge video steganography methods and their performance evaluations from literature. Both compressed and raw video steganographic methods are surveyed. In the compressed domain, video steganographic techniques are categorized according to the video compression stages as venues for data hiding such as intra frame prediction, inter frame prediction, motion vectors, transformed and quantized coefficients, and entropy coding. On the other hand, raw video steganographic methods are classified into spatial and transform domains. This survey suggests current research directions and recommendations to improve on existing video steganographic techniques.**

***Keywords—Video Steganography; Compressed domain; Raw domain; Imperceptibility; Embedding Payload; Robustness***

## I. INTRODUCTION

Steganography is a process that involves hiding important information (message) inside other carrier (cover) data to protect the message from unauthorized users. The mixed data (stego objects) will be seen by the Human Visual System (HVS) as one piece of data because the HVS will not be able to recognize the small change that occurs in the cover data. Message and cover data could be any type of data format such as text, audio, image, and video [1]. The development of steganalysis tools weakens unsecure steganography schemes and rendering them useless. Hence, researchers have to develop secure steganography algorithms that are protected from both attackers and steganalysis detectors. Any successful steganography system should consider three main important factors: embedding capacity, imperceptibility, and robustness against attacks [2].

First, the embedding payload is defined as the amount of secret information that is going to be embedded inside the cover data. The algorithm has a high embedding payload if it has a large capacity for the secret message. The embedding efficiency includes the stego visual quality, security, and robustness against attackers. Second, both a low modification rate and good quality of the cover data lead to a high embedding efficiency. The steganography algorithm that contains a high embedding efficiency will reduce attacker suspicion of finding hidden data and will be quite difficult to detect through steganalysis tools. However, any distortion to the cover data after the embedding process occurs will increase the attention of attackers . The embedding efficiency is directly affected by the security of the steganographic scheme [3]. In traditional steganographic schemes, embedding payload and embedding efficiency are opposite. Increasing the capacity of the secret message will decrease the quality of stego videos that then weakens the embedding efficiency. Both factors should be considered. The deciding factors depend on the steganography algorithm and the user requirements. To improve steganographic schemes, many of the algorithms use matrix encoding and block code principles such as Hamming, BCH, and Reed-Solomon codes [4].

Third, robustness is another factor which measures the steganography algorithm's resistance against signal processing and attacks. Signal processing operations include compression, geometric transformation, filtering, and cropping. The algorithm is robust when the receiver side extracts the secret message correctly, without any errors. High efficient steganography algorithms are robust against both signal processing and adaptive noises [5].

In this article, we review the problem of secure transmission over the public network “Internet” using video steganography, where secret information is embedded in both raw and compressed videos. Video steganography is currently a very enthusiastic field of research, as it offers the promise of overcoming some of the inherent limitations of cryptographic methods such as huge computational complexity and scrambled form of cipher, attracting the attention of attackers, resulting in modification or decryption of secret data.

Recently, a large number of video steganography techniques have been proposed in the literature. Unfortunately, the literature of video steganography lacks survey articles. Therefore, it is realized to present an extensive study of all video steganography techniques for the past decade. The current paper provides a comprehensive survey and analysis of the state-of-the-art video steganographic methods in both compressed and raw domains. In addition, this survey not only investigates the existing video steganographic techniques but also provides recommendations and future directions to enhance those methods. We hope that our contribution will further enrich the

**78•1-4799•6776•6115/$31.00 ©2017 IEEE**

literature of information security in general and video steganography in particular.

The remainder of this paper is organized as follows: Section 2 presents steganography versus cryptography and watermarking. Section 3 discusses video steganography techniques in both raw and compressed domains. Section 4 introduces performance assessment metrics. Section 5 contains the conclusion and some recommendations for future research directions.

## II. Steganography versus Cryptography and Watermarking

The common objective of both steganography and cryptography is to provide confidentiality and protection of data. The steganography "protected writing" establishes a covert communication channel between legitimate parties; while the cryptography "secret writing" creates an overt communication channel [6]. In cryptography, the presence of the secret data is recognizable; however, its content becomes unintelligible to illegitimate parties. In order to increase additional levels of security, steganography and cryptography can operate together in one system [7, 8].

Digital watermarking techniques use a preservation mechanism to protect the copyright ownership information from unauthorized users. This process is accomplished by concealing the watermark information into overt carrier data [9]. Like steganography, watermarking can be used in many different applications such as content authentication, digital fingerprints, broadcast monitoring, copyright protection, and intellectual property protection [10]. Different watermarking techniques can be found in the literature. Fig. 1 clarifies the hierarchy of the overall system security including video steganography, which is the main focus of this survey.

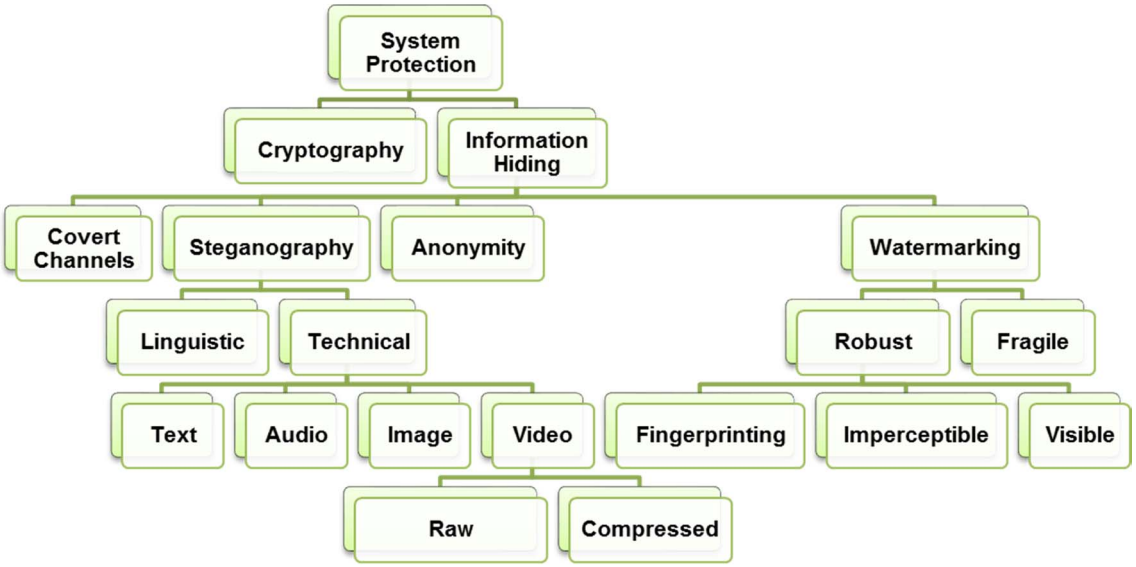


Fig. 1. Disciplines of overall system protection.

## III. Video Steganography Techniques

Due to the advancement of Internet and multimedia technologies, digital videos have become a popular choice for data hiding. The video data contains a massive amount of data redundancy which can be utilized for embedding secret data. Recently, there are many useful applications of video steganography techniques such as video error correcting, military services , bandwidth saving, video surveillance, and medical video security . Video steganography techniques are classified into compressed and uncompressed domains.

### A. *Video steganography techniques in compressed domain*

The H.264 standard has increased the efficiency of video compression when compared to the previous versions. Some new features of H.264 video codec include flexible macroblock ordering, quarter-pixel interpolation, intra prediction in intra frame, deblocking filtering post-processing, and multiple frames reference capability [11]. Usually, H.264 codec comprises a number of group of pictures (GOP). Every GOP includes three types of frames: intra (I) frame, predicted (P) frame, and bidirectional (B) frame. During the video compression process, the motion estimation and compensation processes minimize the temporal redundancy. Since the video stream is a number of correlated still images, a frame can be predicted by using one or more referenced frames based on the motion estimation and compensation techniques. First, frames are divided into 16x16 macroblocks (MB) wherein each MB contains blocks that may include the smallest size of 4x4. When applying a few searching algorithms, block $C$ in the present frame is compared, individually, to one of the selected block $\tilde{R}$ in the referenced frame $\tilde{F}$ in order to find a corresponding block $C$. The prediction error between two blocks ($C$ and $\tilde{R}$) of size b can be measured using Sum of Absolute Differences (SAD).

$$e = SAD(C, \tilde{R}) = \sum_{1 \le i,j \le b} |c_{i,j} - \tilde{r}_{i,j}| \quad (1)$$

Where $c_{i,j}$ $and$ $\tilde{r}_{i,j}$ refer to block values. The best matched block will have a minimum SAD using $C$'s prediction denoted

by $\tilde{P}$. The motion vector and differential error $D = C - \tilde{P}$ are required for the video coding process.

*1) Intra frame prediction*

During the video compression process, the macroblocks are encoded using a number of intra prediction modes. In H.264 codec, the numbers of intra prediction modes are nine of 4x4 blocks and four of 16x16 blocks. Fig. 2 illustrates intra prediction modes for 16x16 blocks. Also, the High Efficiency Video Coding (*HEVC*) codec can support up to 35 intra prediction modes for each 64x64, 32x32, 16x16, 8x8, and 4x4 block sizes. For data concealing purposes, these modes can be mapped to one or more of secret message bits.

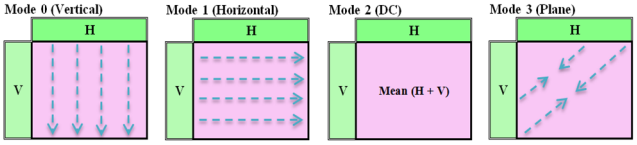


Fig. 2. H.264 intra prediction modes for 16x16 blocks.

*2) Inter frame prediction*

In many video steganographic methods, the seven block sizes that include 16x16, 16x8, 8x16, 8x8, 8x4, 4x8 and 4x4 of H.264 inter frame prediction are commonly utilized as a venue to embed the secret message by mapping each block type to a number of secret bits. Kapotas et al. [12] proposed a data concealing algorithm for scene change detection in H.264 coding. This method uses four different block sizes. Each one is mapped onto one pair of a secret message. In this algorithm, the secret message consists of scene change frames information that will be embedded into the encoded videos. This embedded information will help the scene change detection algorithm, in H.264 video stream, functioning in real time. However, the data hiding methods of the intra frame prediction have a very limited embedding capacity. For example, let "NY" is the secret information that must be embedded into the inter frame prediction blocks in H.264 codec. By using mapping rules of different block sizes the embedding goal can be achieved. Fig. 3 illustrates the embedding process using mapping rules.

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

Mapping

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

Fig. 3. Mapping rules of prediction block type to embed "NY" characters.

*3) Motion vectors*

Motion vector characteristics such as horizontal and vertical components, amplitude, and phase angles are utilized in embedding secret information. Xu et al. [13] proposed a compressed video stream steganography. In this scheme, the embedding process relies on I, P, and B frames. First, the hidden data is concealed into the motion vectors of, both, P and B frames. Only the motion vectors that have high magnitudes are chosen. Here, each macroblock has a motion vector; however, the selected macroblocks are moving rapidly. Secondly, the control information is embedded into I frames. This control information includes the capacity payload and segment range of each GOP. Each GOP contains one I frame which carries the control information necessary for the data extraction phase. In addition, each GOP has a number of P and B frames which contain secret messages in their high magnitude motion vectors. Xu et al.'s method has a low embedding payload because it only used the motion vectors with a high magnitude.

*4) Transform coefficients*

Discrete Cosine Transform (DCT), Quantized DCT (QDCT), and Discrete Wavelet Transform (DWT) coefficients of the luminance component are also good candidates to conceal the secret message due to their low, middle, and high frequency coefficients for data embedding. Huang et al. [14] presented reliable information bit hiding using the DCT and communication theory. In order to enhance the robustness of this method, the BCH codes and soft-decision decoding have been used. Moreover, the robustness is also achieved by testing both the common signal processing operations and a StirMark attack. The secret data is hidden into the DCT coefficients, especially, in DC with the highest energy coefficient and low-frequency AC coefficients. Barni et al. [15] presented a watermarking technique of MPEG-4 video coding based on the video object planes. This scheme hides the watermark information into the selected inter and intra macroblocks of each video object. Depending on the computed frequency mask, DCT coefficients that exceeds to the predefined threshold were chosen for the embedding process. Barni's is flexible and easy to use for many applications. Moreover, it is robust against some common signal processing.

*5) Entropy coding CAVLC and CABAC*

During the H.264 compression, Context Adaptive Variable Length Coding (CAVLC) and Context Adaptive Binary Arithmetic Coding (CABAC) entropy coding can be used as host data to carry secret messages within many video steganographic techniques. Ke et al. [16] presented a video steganographic method relies on replacing the bits in H.264 stream. In this algorithm, CAVLC entropy coding has been applied in the data concealing process. The embedding phase can be completed based on the trailing ones sign flag and the level of the codeword parity flag. The sign flag of the trailing ones changes if the embedding bit equals "0" and the parity of the codeword is even. Also, the sign flag changes if the embedding bit equals "1" and the parity of the codeword is odd. Otherwise, the sign flag of the trailing ones does not change. The trailing ones (*TOnes*) are modified as follows:

$$TOnes = \begin{cases} even\ codeword\ ; if\ secret\ bit = 0 \\ odd\ \ codeword\ \ ; if\ secret\ bit = 1 \end{cases} \quad (2)$$

The modification of high frequency coefficients does not have an impact on the video quality. However, the embedding capacity is low because Ke et al.'s method is established on the non-zero coefficients of the high frequencies that consist of a large majority of zeros.

B. *Video steganography techniques in raw domain*

Unlike the compressed video, raw video steganographic techniques deal with the video as a sequence of frames with the same format. First, digital video is converted into frames as still images, and then each frame is individually used as carrier data to conceal the hidden information. After the embedding process, all frames are merged together to produce the stego video. Raw video steganographic techniques consist of spatial and transform domain techniques [17].

*1) Spatial domain methods*

There are many steganographic techniques that rely on the spatial domain such as LSB substitution, Bit Plane Complexity Segmentation (BPCS), spread spectrum, Region of Interest (ROI), histogram manipulation, matrix encoding, and mapping rule. Basically, these techniques utilize the pixel intensities to conceal the secret message. Zhang et al. [18] presented an efficient embedder utilizing BCH encoding for data hiding. This embedder hides the covert information into a block of carrier object. The concealing phase is achieved by modifying different coefficients in the input block to set the syndrome values null. This method enhances embedding payload and execution duration compared to others. The error correcting code and steganographic model of this method is shown in the Fig. 4. Zhang et al.'s method modifies the complexity of the algorithm from exponential to linear. On the other hand, Diop et al. [19] presented an adaptive steganography method utilizing the low-density parity-check codes. The method discusses how to reduce the influence of hidden information insertion by this codes. This algorithm demonstrated that the low-density parity-check codes are better for encoding algorithms than other codes. The process of embedding and extraction can be accomplished by Eq. 3 and Eq. 4.

$$S = Embedding\ (I, m) \tag{3}$$

$$m = Extraction\ (m) = HS \tag{4}$$

Where $I$ and $S$ are the cover data and steganogram, respectively, and $m$ is a secret message ($m \in F_2^m$).

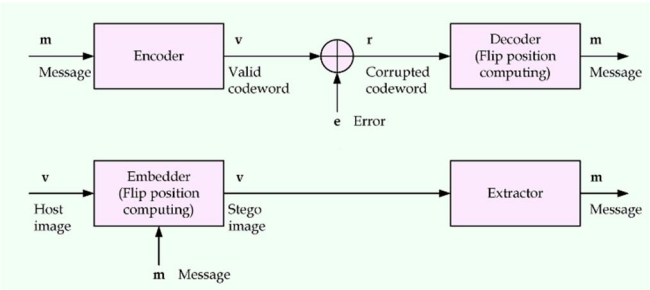


Fig. 4. Error correcting code and steganographic model.

*2) Transform domain methods*

In the transform domain steganographic methods, each video frame is individually transformed into frequency domain using DCT, DWT, and discrete Fourier transform (DFT) and the secret message is embedded utilizing the low, middle, or high frequencies of the transformed coefficients. Patel et al. [20] presented a new data hiding method using the lazy wavelet transform (LWT) technique, where each video frame is divided into four sub-bands, separating the odd and even coefficients. The secret information is then embedded into the RGB LWT coefficients. For accurate extraction of embedded data, the length of hidden data is concealed into the audio coefficients. The amount of hidden information is high, but this type of wavelet is not a real mathematical wavelet operation. Consequently, Patel et al.'s method will not protect the hidden information from attackers.

Table 1 summarizes video steganographic methods that utilize compressed and raw domains for data hiding, highlighting each of embedding capacity, video quality, robustness against attacks, video preprocessing, and secret messages preprocessing.

## IV. Performance Assessment Metrics

The main purpose of steganography techniques is to conceal the secret information inside the cover video data, thus the quality of the cover data will be changed ranging from a slight modification to a severe distortion. In order to evaluate whether the distortion level is acceptable or not, statistically, different metrics have been utilized. Pick Signal to Noise Ratio (*PSNR*) is a common metric utilized to calculate the difference between the carrier and stego data. The *PSNR* can be calculated as follows [21, 22]:

$$MSE = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n}\sum_{k=1}^{h}[C(i,j,k) - S(i,j,k)]^2}{m \times n \times h} \tag{5}$$

$$PSNR = 10 * Log_{10}\left(\frac{{MAX_C}^2}{MSE}\right) \quad (dB) \tag{6}$$

*C* and *S* represent the carrier and stego frames. Both m and *n* indicate the frame resolutions, and *h* represents the RGB colors (*k*=1, 2, and 3).

On the other hand, the performance of steganographic method in terms of embedding capacity is a major factor that any method tried to increase it with the respect of the visual quality. According to [23], any steganographic method has a high hiding capacity if the hidden ratio exceeds 0.5%. The hiding ratio (*HR*) is calculated in the following formula [24]:

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

To further evaluate the performance of any steganographic algorithm in terms of robustness, two objective metrics including bit error rate (*BER*) and similarity (*Sim*) are used. These metrics are applied to determine whether the secret messages are retrieved from the stego videos successfully by comparing the concealed and extracted covert data. The *BER* and *Sim* are computed in the following formulas [25, 26]:

$$BER = \frac{\sum_{i=1}^{a}\sum_{j=1}^{b}[M(i,j) \oplus \widehat{M}(i,j)]}{a \times b} \times 100\% \tag{8}$$

$$Sim = \frac{\sum_{i=1}^{a}\sum_{j=1}^{b}[M(i,j) \times \widehat{M}(i,j)]}{\sqrt{\sum_{i=1}^{a}\sum_{j=1}^{b}M(i,j)^2} \times \sqrt{\sum_{i=1}^{a}\sum_{j=1}^{b}\widehat{M}(i,j)^2}} \tag{9}$$

Where $M$ and $\widehat{M}$ are the concealed and extracted hidden data, and, "*a*" and "*b*" are the size of the hidden data.

**Table 1:** Venues, embedding capacity, video quality, robustness, video and message preprocessing of the existing video steganographic methods.

| Method | Domain/venue for data hiding | Embedding capacity | Video quality | Robustness | Video preprocessing | Message preprocessing |
|---|---|---|---|---|---|---|
| Pan *et al.* [27] | Compressed domain/ Motion vectors | Low embedding capacity (at most 4 bits in 6 bits of high amplitude motion vectors and the modification of 2 bits) | Average PSNR is 37.45 dB | Robust against H.264 compression | Not used | Not used |
| Jue *et al.* [28] | Compressed domain/ Motion vectors | Low embedding capacity (at most 55 bits per P-frame or B-frames macroblocks. Largest amplitude of motion vectors is used) | Average PSNR is 36.27 dB | Robust against H.264/AVC compression | Not used | Not used |
| Barni *et al.* [15] | Compressed domain/ DCT coefficients | Low embedding capacity (at most 30 bits per video object of 500 Kb/s) | Almost the same as compressed video | Robust against MPEG-4 compression | Not used | Not used |
| Li *et al.* [29] | Compressed domain/ DWT coefficients | An average of 38 Kbits per frame of resolution $352 \times 288$ when the first level of DWT is used | Average PSNR is 35.50 dB when the first level of DWT is used | Robust against JPEG/JPEG2000 compression | RIO (object detection by GMM) | Not used |
| Li *et al.* [30] | Compressed domain/ QDCT coefficients | Low embedding capacity (at most 1 bit per $4 \times 4$ luma block) | Average PSNR is 36 dB of Intra frame | Robust against H.264 codec | Not used | Not used |
| Mobasseri *et al.* [31] | Compressed domain/ CAVLC | Low embedding capacity (an average of 1 bit per $8 \times 8$ Intra block) | Almost the same as compressed video | Robust against MPEG-2 encoder | Not used | Not used |
| Wang *et al.* [32] | Compressed domain/ CABAC | Low embedding capacity (1156 bits are embedded in 50 frames of resolution $176 \times 144$) | Almost the same as compressed video (average PSNR is around 37 dB) | Robust against H.264/AVC codec | Not used | Not used |
| Zhang *et al.* [18] | Raw/ Spatial domain | At most the embedding capacity is $m \times t$ bits per $n = 2^m - 1$ bits block, where $m > 2$ and $t = 2$ or 3 | N/A | Not robust against signal processing | Not used | BCH |
| Cheddad *et al.* [33] | Raw / Spatial domain | Average of embedding capacity ratio is 1.03% | Average PSNR is 59.63 dB | Not robust enough against signal processing | Skin region detection | Not used |
| Alavianmehr *et al.* [34] | Raw / Spatial domain | Average of embedding capacity ratio is 1.34% (4096 bits per video) | Average PSNR is 36.97 dB | Robust against H.264/AVC codec | Not used | Not used |
| Hu *et al.* [35] | Raw / Spatial domain | Average of embedding capacity 1.5 bpp | Average PSNR is 29.03 dB | Not robust against signal processing | Not used | Non-uniform Rectangular Partition |
| Sun [36] | Raw / Spatial domain | At most the embedding capacity ratio is 45% | Average PSNR is 44.28 dB | Not robust against signal processing | BPCS | Not used |
| Patel *et al.* [20] | Raw / Transform domain | Average of embedding capacity ratio is 12.5% | Average PSNR is 31.23 dB | Not robust against signal processing | Not used | Encryption |
| Spaulding *et al.* [37] | Raw / Transform domain | Average of embedding capacity ratio is 25% | Average PSNR is 33 dB | Robust lossy compression | BPCS | Not used |

## V. Conclusion and Recommendations

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

- Proposing a video steganographic method that maintains a trade-off between video quality, hiding capacity, and robustness against attacks, this makes it more appropriate for real-time security methods.
- Suggesting a steganographic technique that combines steganography with other system protection methods such as cryptography and error correcting codes.
- Providing a video steganographic algorithm that focuses on a portion of video such as ROI for data embedding process instead of using entire video.

## References


[1] R. J. Mstafa and K. M. Elleithy, "A video steganography algorithm based on Kanade-Lucas-Tomasi tracking algorithm and error correcting codes," *Multimedia Tools and Applications,* pp. 1-23, 2015.

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

[3] W. Jyun-Jie, C. Houshou, L. Chi-Yuan, and Y. Ting-Ya, "An embedding strategy for large payload using convolutional

embedding codes," in *ITS Telecommunications (ITST), 2012 12th International Conference on*, 2012, pp. 365-369.

[4] 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.

[5] R. J. Mstafa and K. M. Elleithy, "A high payload video steganography algorithm in DWT domain based on BCH codes (15, 11)," in *Wireless Telecommunications Symposium (WTS)*, 2015, pp. 1-8.

[6] W. Abu-Marie, A. Gutub, and H. Abu-Mansour, "Image Based Steganography Using Truth Table Based and Determinate Array on RGB Indicator," *International Journal of Signal and Image Processing,* vol. 1, pp. 196-204, 2010.

[7] R. Das and T. Tuithung, "A novel steganography method for image based on Huffman Encoding," in *Emerging Trends and Applications in Computer Science (NCETACS), 2012 3rd National Conference on*, 2012, pp. 14-18.

[8] R. T. Mercuri, "The many colors of multimedia security," *Communications of the ACM,* vol. 47, pp. 25-29, 2004.

[9] A. Khan and S. A. Malik, "A high capacity reversible watermarking approach for authenticating images: Exploiting down-sampling, histogram processing, and block selection," *Information Sciences,* vol. 256, pp. 162-183, 2014.

[10] S.-J. Horng, D. Rosiyadi, P. Fan, X. Wang, and M. K. Khan, "An adaptive watermarking scheme for e-government document images," *Multimedia Tools and Applications,* vol. 72, pp. 3085-3103, 2014.

[11] T. Shanableh, "Data Hiding in MPEG Video Files Using Multivariate Regression and Flexible Macroblock Ordering," *Information Forensics and Security, IEEE Transactions on,* vol. 7, pp. 455-464, 2012.

[12] S. K. Kapotas and A. N. Skodras, "A new data hiding scheme for scene change detection in H. 264 encoded video sequences," in *2008 IEEE International Conference on Multimedia and Expo*, 2008.

[13] C. Xu, X. Ping, and T. Zhang, "Steganography in compressed video stream," in *Innovative Computing, Information and Control, 2006. ICICIC'06. First International Conference on*, 2006, pp. 269-272.

[14] J. Huang and Y. Q. Shi, "Reliable information bit hiding," *Circuits and Systems for Video Technology, IEEE Transactions on,* vol. 12, pp. 916-920, 2002.

[15] M. Barni, F. Bartolini, and N. Checcacci, "Watermarking of MPEG-4 video objects," *Multimedia, IEEE Transactions on,* vol. 7, pp. 23-32, 2005.

[16] N. Ke and Z. Weidong, "A video steganography scheme based on H. 264 bitstreams replaced," in *4th IEEE International Conference on Software Engineering and Service Science (ICSESS)*, 2013, pp. 447-450.

[17] K. Muhammad, M. Sajjad, I. Mehmood, S. Rho, and S. Baik, "A novel magic LSB substitution method (M-LSB-SM) using multi-level encryption and achromatic component of an image," *Multimedia Tools and Applications,* pp. 1-27, 2015/05/24 2015.

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

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

[20] K. Patel, K. K. Rora, K. Singh, and S. Verma, "Lazy Wavelet Transform Based Steganography in Video," in *Communication Systems and Network Technologies (CSNT), 2013 International Conference on*, 2013, pp. 497-500.

[21] K. Muhammad, J. Ahmad, M. Sajjad, and M. Zubair, "Secure Image Steganography using Cryptography and Image Transposition," *arXiv preprint arXiv:1510.04413,* 2015.

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

[23] L. Tse-Hua and A. H. Tewfik, "A novel high-capacity data-embedding system," *IEEE Transactions on Image Processing,* vol. 15, pp. 2431-2440, 2006.

[24] R. J. Mstafa and K. M. Elleithy, "A New Video Steganography Algorithm Based on the Multiple Object Tracking and Hamming Codes," in *2015 IEEE 14th International Conference on Machine Learning and Applications (ICMLA)*, 2015, pp. 335-340.

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

[26] R. J. Mstafa and K. M. Elleithy, "A DCT-based robust video steganographic method using BCH error correcting codes," in *2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT)*, 2016, pp. 1-6.

[27] F. Pan, L. Xiang, X.-Y. Yang, and Y. Guo, "Video steganography using motion vector and linear block codes," in *Software Engineering and Service Sciences (ICSESS), 2010 IEEE International Conference on*, 2010, pp. 592-595.

[28] W. Jue, Z. Min-Qing, and S. Juan-Li, "Video steganography using motion vector components," in *Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on*, 2011, pp. 500-503.

[29] G. Li, Y. Ito, X. Yu, N. Nitta, and N. Babaguchi, "Recoverable privacy protection for video content distribution," *EURASIP Journal on Information Security,* vol. 2009, p. 4, 2009.

[30] Y. Li, H.-x. Chen, and Y. Zhao, "A new method of data hiding based on H. 264 encoded video sequences," in *Signal Processing (ICSP), 2010 IEEE 10th International Conference on*, 2010, pp. 1833-1836.

[31] B. G. Mobasseri and M. P. Marcinak, "Watermarking of MPEG-2 video in compressed domain using VLC mapping," in *Proceedings of the 7th workshop on Multimedia and security*, 2005, pp. 91-94.

[32] R. WANG, L. HU, and D. XU, "A Watermarking Algorithm Based on the CABAC Entropy Coding for H.264/AVC," *J. Comput. Inform. Syst.,* vol. 7, no. 6, pp. 2132–2141, 2011.

[33] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "A skin tone detection algorithm for an adaptive approach to steganography," *Signal Processing,* vol. 89, pp. 2465-2478, 2009.

[34] M. A. Alavianmehr, M. Rezaei, M. S. Helfroush, and A. Tashk, "A lossless data hiding scheme on video raw data robust against H.264/AVC compression," in *2012 2nd International eConference on Computer and Knowledge Engineering (ICCKE)*, 2012, pp. 194-198.

[35] S. Hu and U. KinTak, "A Novel Video Steganography based on Non-uniform Rectangular Partition," in *Computational Science and Engineering (CSE), 2011 IEEE 14th International Conference on*, 2011, pp. 57-61.

[36] S. Sun, "A New Information Hiding Method Based on Improved BPCS Steganography," *Advances in Multimedia,* vol. 2015, 2015.

[37] J. Spaulding, H. Noda, M. N. Shirazi, and E. Kawaguchi, "BPCS steganography using EZW lossy compressed images," *Pattern Recognition Letters,* vol. 23, pp. 1579-1587, 2002.