IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol.-6, Issue-5, May 2018 E-ISSN: 2347-2693

H.264/AVC Video Steganography Techniques: An Overview

Mukesh Dalal*, Mamta Juneja

[1,2] UIET, Panjab University, Chandigarh, India

*Corresponding Author: mukeshdalal05@gmail.com

Available online at: www.ijcseonline.org

Accepted: 21/May/2018, Published: 21/May/20182018

***Abstract*—** Video steganography is a process of embedding data inside in a raw or compressed video sequence. Nowadays compressed videos are preferred over raw videos for data transfer, and H.264/ AVC video format is the most frequently used video standard over the internet. H.264/AVC provides more compression as compared to the previous standards and maintains better visual quality. In H.264/ AVC video steganography the message hiding can be done by conventional methods such as spatial domain and transform domain techniques. Additionally, it has more hiding options as compared to the previous standards which are also utilized by researchers for secret data embedding. In this paper, a concise overview of H.264/ AVC video standard is given, and survey of existing video steganography techniques in H.264/ AVC is also done with the implementation of a 4-0-4 LSB technique to show the impact of embedding. The pros and cons of different hiding techniques used for data embedding in H.264/AVC video are discussed towards the end. This paper aims to provide a brief introduction of video steganography techniques in H.264/ AVC video coding standard.

***Keywords*—**Video Steganography, H.264/AVC, Motion vector, Entropy Coding, DCT, Spatial domain, Transform domain

I. INTRODUCTION

The advancement of technology has made the communication easy and fast because of the use of internet nowadays. However, the information travels through unsecured communication channels, and there are chances of getting confidential data interrupted in between and in the worst case it can even harm the national security. So to improve the confidentiality and security of the secret message steganography are used where the secret information can be hidden inside the multimedia file without any knowledge to the intruders. In steganography, only the sender and the recipient know about the secret message transfer, and it is even more secure than cryptography where ciphertext attracts the intruder to decode the data. Steganography can be done by hiding the secret message in text, audio, image and video file. There are three fundamental requirements for a successful steganography technique: hiding capacity, imperceptibility, and robustness. Although these three requirements are necessary for a good steganography technique, however, they have an impact on each other. As the capacity increases, the quality of the stego-object decreases resulting in low imperceptibility, also it can affect the robustness of the stego-object. Nowadays, due to the frequent transfer and easy access to videos, it has become a new hotspot for steganography. The size of the video is large as compared to the image, so it provides more options for hiding the secret message in it. Video steganography is more robust and secure because of its complex statistical structure which makes it hard to detect. Block diagram of basic video steganography is shown in Figure 1 where at sender's side the video sequence is taken as input and the secret data/message is embedded in it with the help of some embedding algorithm and sent through the transmission channel. At receiver's side, the stego-video is processed through extraction algorithm which extracts the secret data from the video sequence. This aim of this paper is to give a brief introduction of some latest H.264/AVC video steganography techniques aiming to give an overview to the new researchers to initiate their research in this field.

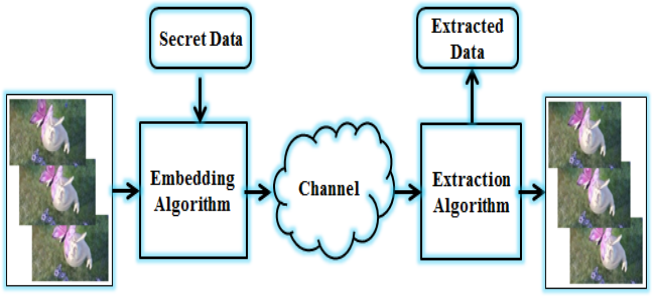

Figure 1 Steganography block diagram

The rest of the paper is tied as follows: Section II presents the H.264/ AVC standard introduction and in section III, a 4-0-4 LSB technique is discussed with the visual results and steganography techniques related to H.264/AVC is also discussed with their pros and cons. In section IV future

recommendations are given and section V concludes the paper.

II. H.264/AVC STANDARD

H.264/AVC is a motion- compensated and block oriented video compression standard and is also known as MPEG-4 Part 10. It is the most frequently used video coding standard for compression, recording, and transfer of the video content till date. H.264/AVC was originated by the alliance of the ITU-T Video Coding Experts Group (VCEG), Joint Video Team (JVT), and the ISO/IEC JTC1 Moving Picture Experts Group(MPEG). In May 2003, the first version of this video standard was accomplished and after that different expansion of its capabilities have been appended in later editions [1][2].

As previous standards have the basic encoding steps: transformation, quantization, motion compensated prediction and entropy coding H.264/AVC standard also has all these essential elements. Additionally, H.264/AVC has some more important features as intra-prediction mode, 4x4 integer transform, variable block sizes (16x16, 8x16, 16x8, 8x8, 4x8, 8x4, 4x4), several reference frames, a quarter-pixel precision for motion compensation and better entropy coding [2]. The necessary steps in encoding an H.264/ AVC video are shown in Figure 2. The video frames are split into different blocks using variable block size, and the block is predicted based on its neighboring blocks (also past frames or future frames). The actual pixel data is used to subtract the prediction to get the residual, and this residual data is transformed with the help of integer DCT. The coefficients of integer DCT are than quantized and at last entropy coding are done to convert it into a bit-stream.

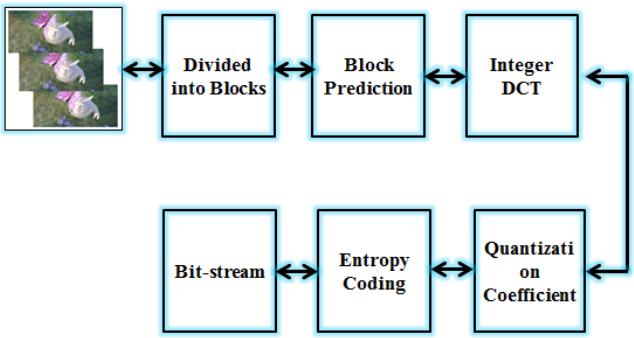

Figure 2 Video Encoding Block-Diagram

In H.264/AVC three kinds of frames are there: I (Intra) frame, P (Predicted) frame and B (Bi-directional predicted) frame. The intra-prediction (I- frame) is the one which are independent images which use the same frame for prediction. P frames are the prediction frames using only one motion vector by referring to a past frame. B frames are the prediction frames using two motion vectors by referring the past as well as future frames. The frames intra and inter-predicted is not encoded in the display sequence. The I, P and B frames concatenation is known as Group of Pictures (GOP) which is formed by the combination of these frames, an example is shown in Figure 3. The frames and macroblocks can be further split into slices which can be again divided into I, P or B type and they can be interpreted independently [3].

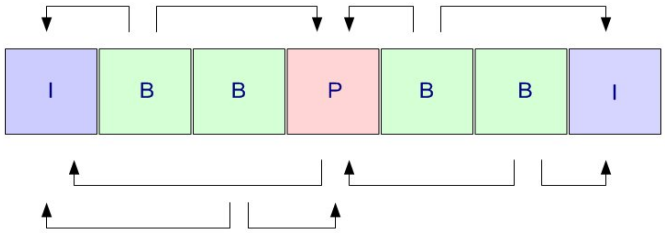

Figure 3 Example of GOP (IBBPBBI)

H.264/AVC has additional features which help in enhancing the coding efficiency of the standard [4], some of them are utilized by researchers for embedding secret data which are discussed below:

- **Variable block size**: H.264/AVC provides more block sizes for motion compensation as compared to the previous standards which include 4x4, 8x8, 4x8, 8x4, 16x16, 8x16, 16x8, etc.
- **Multiple reference pictures/frames**: The standard provides multiple reference frames which allow the encoder to select reference frame among multiple frames for motion compensation.
- **Small (4x4) block size transform:** In H.264/AVC the primary block size for transform is 4x4 which is smaller than previous standards where 8x8 was used for the transform. This small size block represents the signals in a locally adaptive manner which helps in reducing ringing artifacts.
- **Hierarchical block transforms:** The standard provides hierarchical block transform which enables in two modes: 1) by extending the active block size to 8x8 for low frequency chroma information, and 2) by extending the length of the luma transform to a 16x16 block size for low-frequency information for intra coding.
- **Context Adaptive coding:** The H.264/AVC standard enables two types of context adaptive entropy encoding to improve the performance namely, context adaptive variable length coding

(CAVLC) and context adaptive binary arithmetic coding.

- **FMO (Flexible macroblock ordering):** The frame is partitioned into regions known as slice groups where each slice can be an independently decodable subset for the slice group.

The H.264/AVC standard has many more additional features which can be utilized for different purposes. The next section describes the steganography techniques present in the literature using H.264/AVC video coding standard as a cover video.

III. METHODOLOGY

The primary classification for steganography based on the domain is the spatial and transform domain as shown in Figure 4 and researchers utilized the techniques of both the domains for embedding a secret message in H.264/AVC videos.

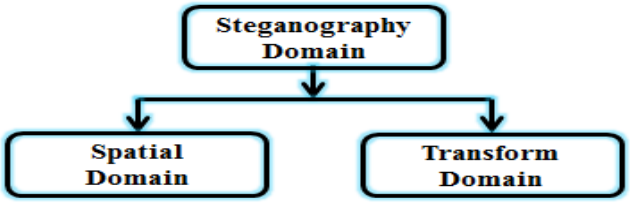

Figure 4 Domains of steganography

LSB (Least Significant Bit) embedding is one of the most fundamental techniques of spatial domain utilized for secret data embedding [5][6]. In this, the LSB bits of the video frames are replaced by the bits of secret data without distorting the quality of the cover video [7]. Generally in LSB replacement, last 4 bits can be replaced with secret data bits without distortion. The embedding can be done in RGB components of the frame where R-represents red, G-represents green and B-represents the blue color component.

The authors implemented a 4-0-4 LSB embedding scheme to show the effect of video steganography on video frames and how basic embedding is done. The H.264/AVC video standard with baseline profile is utilized for embedding and is taken as input to extract the frames from that video. The embedding is done in the frames of the video by replacing last 4 bits of Red and Blue component as shown in Fig 5. Green component remained unchanged as the human eye is most sensitive to green color, keeping that as a priority only red and blue components were chosen for embedding. While embedding, the secret data is first converted into bits and first four bits of the secret message are hidden in LSB of red component and last four bits are hidden in blue component LSBs.

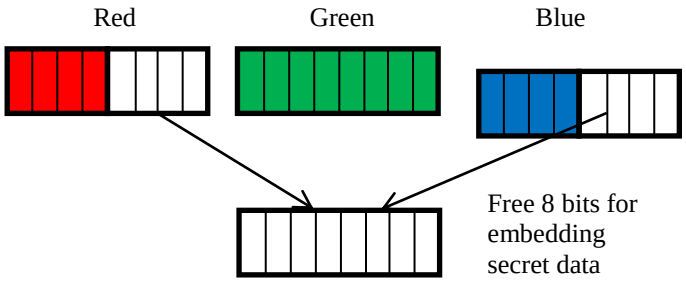

Figure 5 Each RGB pixel hiding capacity in 4-0-4 LSB

The steps for embedding are given below:

i) Input video.
ii) Extract frames from the video.
iii) Convert the frame into R, G and B components.
iv) Embed the secret message (*.txt) into red and blue components using LSB 4-0-4 replacement.
v) Reassemble the stego-frames to generate stego-video.

The steps from extraction are in given below:

i) Input stego-video.
ii) Extract the stego-frames from the video.
iii) Convert the frame into R, G and B components.
iv) Extract the secret message from the red and blue components.
v) Reassemble the frames to generate the original video.

The results of this technique illustrated that the secret data is hidden and extracted without any visual distortion with PSNR 76.2929. The visual results of this technique are shown in Figure 6 and the histogram was generated for the first frame of the cover and stego-video as shown in Figure 7 which shows that there is no clear difference between the cover and stego-video frame.

Figure 6 (a) Original frame

Figure 6 (b) Stego frame

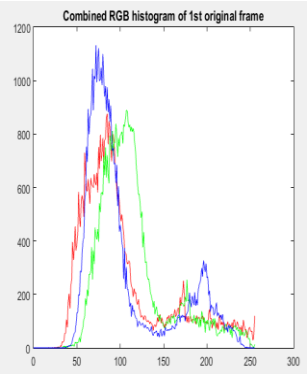

Figure 7 (a) Histogram of the original frame

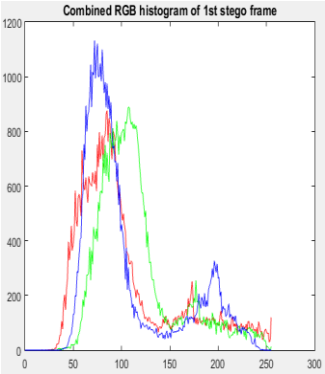

Figure 7 (b) Histogram of stego-frame

LSB is the simplest and the fastest method of embedding data in a video, but this method is not robust due to which it is more prone to attacks. For robust video steganography, temporal domain techniques can be utilized such as DFT, DCT, and DWT [8]. In these techniques, embedding is done in the transformed coefficients of the video/frames which make it more robust and highly secure without any visual distortion. Some of the researchers utilized motion vectors for embedding the data and few of the researcher's utilized entropy encoding techniques for video steganography which are discussed in this section. The categorization is done according to the literature available on video steganography in H.264/AVC standard.

A. Intra Prediction

In H.264/ AVC video steganography intra-prediction mode is utilized for embedding the data where the prediction is carried out in the spatial domain where previously coded blocks are used as a reference for prediction. The reference blocks are the neighboring blocks which are above and left of the predicted block, and due to this, the prediction is allowed individually from intra coded neighboring macroblocks [9].

Ma et al. [10] presented a data hiding scheme in DCT coefficients of 4x4 macroblock luma components and the aim was to embed data inside the cover video without intra-frame distortion drift. The proposed scheme utilized pair of coefficients for embedding process as one of them was used for embedding and the other one was used to mend the level of distortion. The results demonstrated that this scheme was able to achieve high PSNR and utilized 46% of the total 4x4 luma blocks for embedding.

Esen et al.[11] presented a forbidden zone hiding scheme to embed secret data for robustness and imperceptibility trade-off. This scheme utilized the concept of the forbidden zone for the selection of zones and partitions for embedding where no modification was allowed and the formula used for this isshown below.

$$X = \begin{cases} s, & s \in FZ_m \\ M_m(s), & M_m \in AZ_m \end{cases} \quad (1)$$

Where 'X' is the marked signal, 's' is host signal, 'Mm' represents the mapping function, and a pair of FZm and AZm defines the signal where no modification is allowed. The data was embedded by utilizing middle frequency components of DCT transform of the luminance (Y) component of the frame. The results obtained showed that the scheme was able to achieve high PSNR and to ensure robustness this scheme was tested on some common video processing attacks.

Liu et al.[12] presented a data hiding scheme by utilizing DCT coefficients in I frames and for that 4x4 luminance block was utilized. Before embedding the secret data was processed using BCH (n,k,t) codes to ensure robustness of the technique. The results demonstrated that BCH (63,7,15) was the best-concerning robustness and the proposed scheme was able to achieve a high payload with good visual quality with PSNR above 35 dB.

Liu et al. [13] proposed a scheme to prevent intra-frame distortion drift and for that integer, discrete cosine transformation(IDCT) coefficients were utilized for embedding process. The secret message was first partitioned into sub-parts with the help of matrix equation by utilizing Shamir's (t,n) threshold for secret sharing to make it more robust. The results indicated that the proposed scheme was able to recover the original video after extraction and maintain a good quality of the stego-video with average PSNR 36.5 dB.

B. Motion Vector

In intra-frame prediction mode, video steganography motion vector based embedding used where secret data is embedded by altering the motion vector components. Generally, the first step is to find the suitable motion vector using some algorithm or selection rules and after that, the embedding is done in the selected motion vectors. The benefit of using motion vector is that it is not prone to quantization noise as the data is encoded losslessly [14].

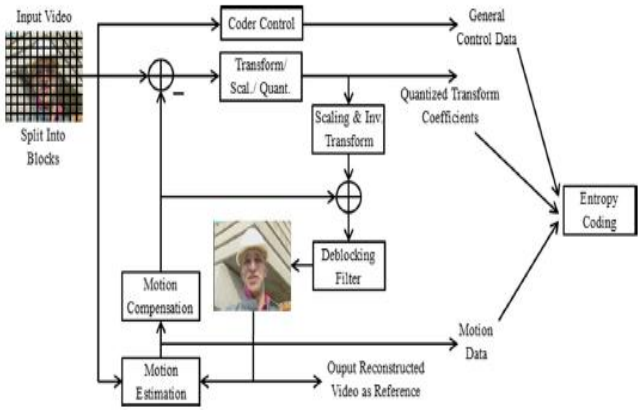

Figure 8 Structure of inter-coded macroblock [15]

Zhu et al. [16] presented a scheme for hiding data in quarter-pixel of motion estimation by using the modulation process which helps in searching the embedding pixels. The quarter pixel search graph is shown below in Figure 9. This scheme introduces rate-distortion cost while embedding the data which resulted in maintaining the video quality after embedding. The results showed that this scheme was able to hide data without affecting the video quality and bit rate with high embedding capacity.

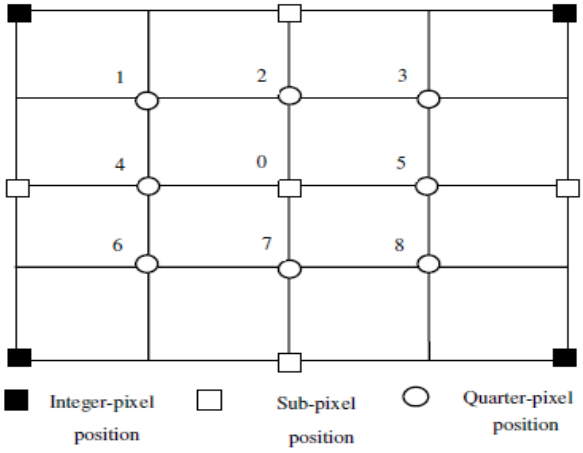

Figure 9 Quarter-pixel ME (motion estimation) search graph [16]

Jue et al. [17] proposed a video steganography technique for embedding data in H.264/AVC videos motion vector components. This scheme designed an algorithm for embedding by calculating the mod difference between the motion vector components (horizontal –vertical). Embedding was done in P and B macro-blocks, and the results indicated that this scheme provides high capacity without any visual distortion and the scheme was fast and easy to implement.

Yao et al. [15] proposed a distortion function scheme by using the two changes which occur after motion vector embedding process. One of the change is the prediction error change (PEC) and the other one is statistical distribution change (SDC) by utilizing two-layered STCs (syndrome-trellis Codes) based ± 1 embedding. The proposed scheme was tested against two existing steganalysis techniques and the results indicated that this scheme was able to achieve high PSNR value to ensure imperceptibility. Cao et al. [18] also presented another scheme of syndrome-trellis code(STC) and for embedding, perturbations were presented during ME process. This scheme was tested against many steganalysis algorithms resulted in a more secure video steganography technique and was able to achieve a better visual quality.

C. Entropy Encoding

In H.264/AVC coding after IDCT for 4x4 blocks and zig-zag order scanning, entropy encoding mode is there. In H.264/ AVC there are two entropy coding modes: CAVLC and CABAC. In Context Adaptive Variable Length Coding (CAVLC), the code-word table is used from which the of non-zero coefficients number is chosen from the neighboring blocks. In Context Adaptive Binary Arithmetic Coding (CABAC), a probability distribution function is estimated across coefficients based on formerly discerned data. Few of the researchers utilized the properties of CAVLC for video steganography.

Ke et al. [19] presented a scheme for hiding data in a video stream by utilizing CAVLC entropy encoding feature. This scheme utilized the trailing coefficients parity codes (even or odd) for embedding process in high-frequency coefficients of 4x4 residual blocks. The results demonstrated that this scheme was able to achieve good visual quality and high hiding capacity. An improved technique for hiding data by utilizing CAVLC codeword substitution was presented by Xu et al. [20]. This scheme utilized the multiple-base notational system and paired codeword for embedding the data in an encrypted video to improve the security. This scheme enhanced the hiding capacity by preserving the visual quality of the stego-video.

D. Hybrid Embedding

Some of the researchers utilized the features of different hiding options together such that motion vectors, quantization parameters, macroblocks, etc. for embedding the data in H.264 videos.

Su et al. [21] presented a scheme with three profiles high, medium and low which utilized different methods of embedding the data. This scheme utilized quantized coefficients, intra-prediction and inter-prediction mode for embedding the data. Embedding was done in quantized coefficients of the prediction residuals and 4x4 intra coding residuals. The results indicated that each profile has some features better than others so depending upon the requirement profiles can be chosen.

Xu et al. [22] proposed a scheme for embedding data in H.264/ AVC videos which were encrypted by utilizing code-word substitution. Two entropy encoding techniques were combined with an encryption algorithm. The secret data was embedded in P frames by generating the codewords of MV difference, DCT coefficients, and intra-prediction mode. The results demonstrated that the proposed scheme was able to maintain the bit rate after encryption as well as after embedding.

Yao et al. [23] proposed hiding technique for encrypted H.264 video sequences by utilizing motion vectors, the prediction mode and DCT coefficients. The proposed scheme first analyzed the distortion in frames originated due to embedding and the following inter-frame distortion drift. The video was first encrypted and after that embedding was done using histogram shifting technique. The experimental results indicated that the scheme was able to achieve high visual quality by decreasing the distortion in P-frame.

Table 1 Pros and cons of different embedding techniques utilized for embedding in H.264/AVC.

Technique	Pros	Cons
Intra- Prediction Mode/ 4x4 DCT macro-blocks	Simple and easy way of hiding data.	Generally, result in high bit-rate after embedding.
Inter Prediction Mode/ Motion Vector	Motion Vector embedding is the most frequently used technique as it can hide a large amount of data[14]	Detecting motion vector is a complex task.
Entropy Coding (CAVLC)	Data embedding is simple as data is embedded directly by code-word substitution.	Causes size overhead of video file[1]
Hybrid	Better utilization of spatial and temporal correlation.	Complex in terms of computation as well as time.

IV. FUTURE RECOMMENDATIONS

Video steganography can be done using spatial domain and transform domain techniques for raw videos and compressed videos. Spatial domain techniques are easy and fast to implement and are less complex whereas transform domain techniques are comparatively complex. In most of the practical applications, due to storage limitation videos are used in the compressed form. Over the past decade, H.264/AVC video coding standard is the most commonly used compressed video for steganography. For compressed videos, transform domain techniques are better as they can partially decode the video, embed the secret data and again re-compress it. Transform domain based techniques are more complex and more time consuming but time can be managed by using supercomputers with high computing power. In literature also most of the techniques are based on transform domain based techniques and in future also transform domain must be explored more. The following section provides the future recommendations for an appropriate video steganography technique.

In addition to H.264/AVC, a new and young standard H.265/HEVC is there which has not been utilized much by researchers for video steganography till date. This should be considered for video steganography in future as it contains additional and advanced features as compared to the previous standard which can be used for embedding.

A video steganography technique must be developed which can make a better trade-off between the three basic requirements capacity, imperceptibility, and robustness. A real-time application for video steganography can be attained only by proposing a better technique with all these requirements.

Video steganography should be combined with other techniques to provide better security. As an example, it can be combined with different encryption schemes to encrypt the secret data which gives additional security to the secret data.

Incorporating embedding to the portion of the frame rather than the complete frame will enhance the robustness and security against attacks. Also, embedding to the transformed coefficients of the selected portion rather than the actual pixels will further improve the robustness.

V CONCLUSION

Video steganography is an emerging area in the field of information security, and specifically, H.264/ AVC videos are the best choices for embedding as this is the most accepted video format over the internet nowadays. This study presented an overview of video steganography techniques utilized for hiding a secret message in H.264/AVC video sequences. The encoding process of H.264/AVC has several steps of processing which provide more options for hiding the data inside it. All these hiding options have some features that can be utilized for embedding the data without much distortion. In this paper, a simple 4-0-4 LSB embedding technique is also implemented on H.264/AVC, and the obtained results are without any visual distortion. The existing techniques of H.264/AVC video steganography are also discussed which utilized different features for embedding the secret data with their pros and cons.

REFERENCES

[1] H. A. V. C. C. Video, Y. Tew, and K. Wong, "An overview of information hiding in H. 264/AVC compressed video," *Circuits Syst. Video Technol. IEEE Trans.*, vol. 24, no. 2, pp. 305–319, 2014.

[2] I. E. Richardson, H. 264 and MPEG-4 video compression: video coding for next-generation multimedia. *John Wiley & Sons*, 2004.

[3] A. Neufeld and A. Ker, "A study of embedding operations and locations for steganography in H. 264 video," *IS&T/SPIE Electron. Imaging*, 2013.

[4] T. Wiegand, G. J. Sullivan, G. Bjontegaard, and A. Luthra, "Overview of the H. 264/AVC video coding standard," *IEEE Trans. circuits Syst. video Technol.*, vol. 13, no. 7, pp. 560–576, 2003.

[5] S. Nimje, A. Belkhede, G. Chaudari, A. Pawar, and K. Kharbikar, "Hiding existence of communication using image steganography," *Int. J. Comput. Sci. Eng.*, vol. 2, pp. 163–166, 2014.

[6] S. Suri, H. Joshi, V. Mincoha, and A. Tyagi, "Comparative analysis of steganography for coloured images," *Int. J. Comput. Sci. Eng.*, vol. 2, no. 4, pp. 180–184, 2014.

[7] M. Dalal and M. Juneja, "Video Steganography Techniques in Spatial Domain-A Survey," in *Proceedings of the International Conference on Computing and Communication Systems, Springer, Singapore*, pp. 705–711, 2018.

[8] M. Dalal and M. Juneja, "A robust and imperceptible steganography technique for SD and HD videos," *Multimed. Tools Appl.*, pp. 1–21, 2018.

[9] A. K. Khan and H. Jamal, "The Intra prediction in H. 264," *Nov. Algorithms Tech. Telecommun. Autom. Ind. Electron.*, pp. 11–15, 2008.

[10] X. Ma, Z. Li, H. Tu, and B. Zhang, "A data hiding algorithm for h.264/AVC video streams without intra-frame distortion drift," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 20, no. 10, pp. 1320–1330, 2010.
[11] E. Esen and A. A. Alatan, "Robust video data hiding using forbidden zone data hiding and selective embedding," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 21, no. 8, pp. 1130–1138, 2011.
[12] Y. Liu, Z. Li, X. Ma, and J. Liu, "A robust data hiding algorithm for H.264/AVC video streams," *J. Syst. Softw.*, vol. 86, no. 8, pp. 2174–2183, 2013.
[13] Y. Liu, L. Ju, M. Hu, H. Zhao, S. Jia, and Z. Jia, "A new data hiding method for H.264 based on secret sharing," *Neurocomputing*, vol. 188, pp. 113–119, 2016.
[14] A. Sur, S. V. M. Krishna, N. Sahu, and S. Rana, "Detection of motion vector based video steganography," *Multimed. Tools Appl.*, vol. 74, no. 23, pp. 10479–10494, 2015.
[15] Y. Yao, W. Zhang, N. Yu, and X. Zhao, "Defining embedding distortion for motion vector-based video steganography," *Multimed. Tools Appl.*, vol. 74, no. 24, pp. 11163–11186, 2015.
[16] H. Zhu, R. Wang, and D. Xu, "Information hiding algorithm for H. 264 based on the motion estimation of quarter-pixel," in *Future Computer and Communication (ICFCC), 2010 2nd International Conference on*, vol. 1, pp. V1--423, 2010.
[17] 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*, pp. 500–503, 2011.
[18] Y. Cao, H. Zhang, X. Zhao, and H. Yu, "Covert communication by compressed videos exploiting the uncertainty of motion estimation," *IEEE Commun. Lett.*, vol. 19, no. 2, pp. 203–206, 2015.
[19] N. Ke and Z. Weidong, "A video steganography scheme based on H. 264 bitstreams replaced," in *Software Engineering and Service Science (ICSESS), 2013 4th IEEE International Conference on*, pp. 447–450, 2013.
[20] D. Xu, R. Wang, and Y. Q. Shi, "An improved scheme for data hiding in encrypted H.264/AVC videos," *J. Vis. Commun. Image Represent.*, vol. 36, pp. 229–242, 2016.
[21] P. C. Su, M. T. Lu, and C. Y. Wu, "A practical design of high-volume steganography in digital video files," *Multimed. Tools Appl.*, vol. 66, no. 2, pp. 247–266, 2013.
[22] D. Xu, R. Wang, and Y. Q. Shi, "Data hiding in encrypted H.264/AVC video streams by codeword substitution," *IEEE Trans. Inf. Forensics Secur.*, vol. 9, no. 4, pp. 596–606, 2014.
[23] Y. Yao, W. Zhang, and N. Yu, "Inter-frame distortion drift analysis for reversible data hiding in encrypted H.264/AVC video bitstreams," *Signal Processing*, vol. 128, pp. 531–545, 2016.

Authors Profile

Ms. Mukesh Dalal received her B. Tech degree from JCDV, KUK, Kurukshetra (Haryana) in 2010, in Information Technology, and the M.Tech Degree from CDLU, Sirsa (Haryana) in 2013, in Computer Science and Engineering. Currently, she is pursuing full-time Ph.D. in Computer Science and Engineering at University Institute of Engineering & Technology, Panjab University, Chandigarh. Her research interests include image processing, video processing, steganography and steganalysis.

Dr. Mamta Juneja received her B.Tech and M.E. degree in Computer Science and Engineering. She obtained her Ph.D. degree in 2013 in the field of Image processing. She has been into the teaching profession since 2001 and has published more than 150 papers in refereed International Journals and conference proceedings with more than 550 citations in Google Scholar. She has served as reviewer for many reputed journals. Presently, she is working as an Assistant Professor in the Department of CSE, University Institute of Engineering. & Technology, Panjab University, Chandigarh, India. She is working on various research projects funded by MHRD and DeITY. Her research interests include data hiding, steganography, biometric security, image, video and signal processing.

