Secured Video Steganography in DWT-DCT Domains Based on Multiple Object Tracking using H.264 Algorithm

Laxmi Gulappagol, K.B.ShivaKumar

Abstract*: The technological development in past few years has led to the evolution of new techniques for secured digital data communication. Video steganography is one of the most efficient methods for secure and robust data communication. This article presents a steganographic algorithm in transfer domain using Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT) based on Multiple Object Tracking, encoding and decoding using H.264 algorithm. Initially input video is divided into 'N' number of frames on which motion object detection and tracking is implemented. 2-D DWT is applied on RGB channels of each motion region resulting in LL-LH and HH sub bands. DCT is also applied on the same motion region resulting in DC and AC co – efficient. The resultant stego video is rebuilt by combining non-motion objects and transformed motion objects of the frame. The performance analysis is carried out for Peak Signal to Noise Ratio (PSNR), Correlation, Mean Square Error and SSIM. The effect of attacks such as Gaussian White and Salt & Pepper are also analysed. The experimental results predict that the recommended algorithm improves the embedding capacity and also enhances the robustness of secured data communication.

***Index Terms*: DCT, DWT, Multiple Object Tracking,H.264, Stego Video.**

I. INTRODUCTION

Steganography is a Greek word which means covered writing. It plays a vital role in hiding data in digital videos [1]. Technological development and requirement of efficient and secure sharing of digital data is responsible for video steganography. [2, 3]. In past few years, video steganography has become an effective tool as a large amount of data can be hidden effectively without causing content distortion in which the data is hidden in each video frame independently.However, transparency, robustness, payload capacity and computational complexity of embedding and extracting the hidden data are the important parameters to be considered [4, 5]. H.264/AVC is one of the most commonly adopted video compression formats.It is the advanced standard for compressing video with high compression efficiency. Hence most of the digital video technologies depend on H,264 compression framework. [2, 6-17]. DCT and DWT are the two common methods for hiding data in transform domain.Here the digital data is converted from spatial domain to transform domain. The cover video is transformed using any these algorithms and then embedded in to appropriate co efficient. 2-D DWT is a multi-resolution process that discretises the video frames into horizontal, vertical and diagonal sub-bands by using high and low pass disintegration, where as DCT is applicable for video and image compression and also inserting data of low frequencies of cover image pixels. [9, 15, 18].

II. RELATED WORK

This section presents existing work that have been used related to DWT-DCT domains for H-264/AVC compressed videos prior to the proposed work.

K. Munivara Prasad et al., [1] have proposed a new approach of steganography for handling attacks. The imperceptibility of BCBS algorithm is improved by DCT. The hiding capacity is improved by fractal compression and security is made effective by using DES for encryption.Ma et al., [2] have proposed a innovative readable data hiding algorithm to embed data in to DCT coefficients of I frames without distorting intraframe into H.264/AVC video. K B Shiva Kumar et al., [3] have proposed a new steganographic technique with multiple transformation.Reliability is enhanced by EDCC. Alavianmehr et al., [5] have proposed a lossless data hiding technique by applying Histogram Distribution Constrained (HDC). Exact recovery of the original video is possible with this method for H.264/AVC video compression. Ke et al., [6] have put forth a scheme with Context Adaptive Variable Length Coding (CAVLC) for H.264 baseline entropy coding. Zafar et al., [7] have analysed an approach of data hiding by embedding both in intra and inter frames from H.264/AVC video codec over a vast range of QP values. Extraction of message is made possible by QTCs. Liu et al., [10] have presented a robust readable information hiding algorithm for H.264/AVC video frames without distorting intraframe drift with high visual quality. Mstafa et al., [13] have proposed a new video steganography method in DCT domain based on BCH and Hamming codes. The data is encrypted by BCH codes and then embedded by DCT for both fast- and slow-moving videos. Mstafa et al., [15] have proposed a robust and secure video algorithm in both DWT and DCT domains based on MOT and error correcting codes. Saurabh et al., [17] have put forth a novel technique to hide data in H.264/AVC compressed videos. Initially videos are compressed and F5 algorithm is used improve efficiency and prevent attacks in a better way. Wijaya et al., [18] have

Revised Manuscript Received on March 26, 2019

Laxmi Gulappagol, Research Scholar, Dept.of ECE, VTU, Jnana Sangama, Belgaum, Karanataka, India.

K.B.ShivaKumar, Department of Telecommunication, Sri Siddhartha Institute of Technology, Tumkur, Karnataka, India.

proposed a robust and secure video steganographic algorithm in both DWT and 2D- DCT domains to improve the embedding capacity in to increase PSNR value.

III. PROPOSED METHOD

The proposed technique is a new approach of robust and secured steganographic algorithm in transfer domain using DWT and DCT based on Multiple Object Tracking, encoding and decoding using H.264 algorithm. “N” number of frames are extracted from the selected video. These frames are resized and filtered by using the Gaussian filter and then transformed by using DCT and DWT out of which Low-Low band is selected for the encryption process with the aid of generated key further followed with decryption. The above operation is performed for all the frames of the input video. The sequence of the processes in the proposed method is shown in Fig. 1.

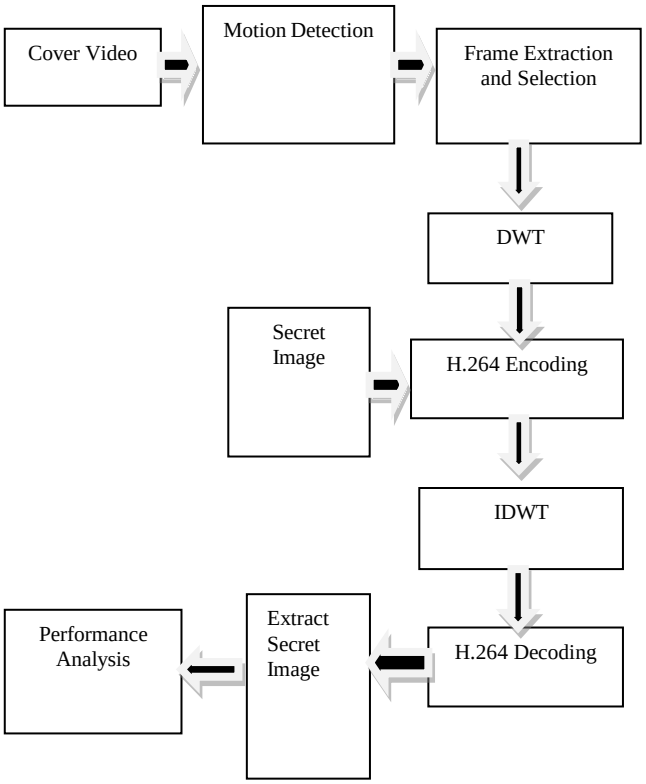


Figure 1. Proposed video steganography frame work.

The proposed steganographic algorithm is structured into two stages: data embedding anddata extraction. The cover video of 256 x 256dimension at 15 frames per second, and data rate 23592 kbps is considered for embedding which is detailed in Fig. 2 and Fig. 3. The secret image is embedded using H.264 algorithm with DCT and DWT transformation.The sequence of embedding Algorithm-1 is detailed further,

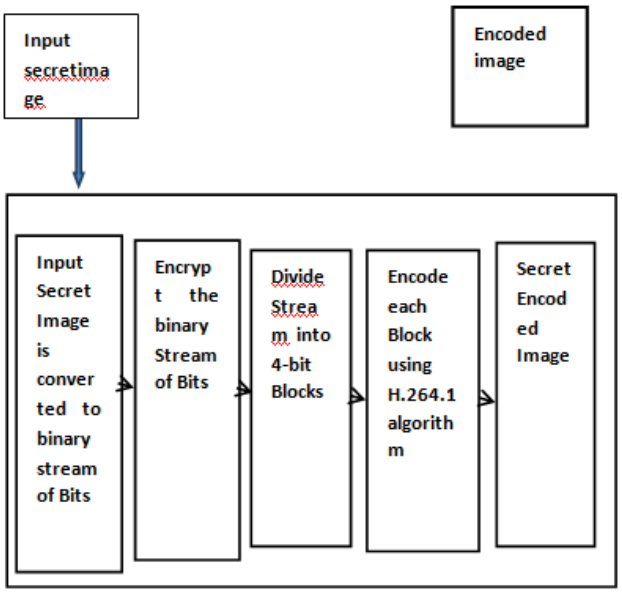


Figure 2. Process of encrypting and encoding input secret image.

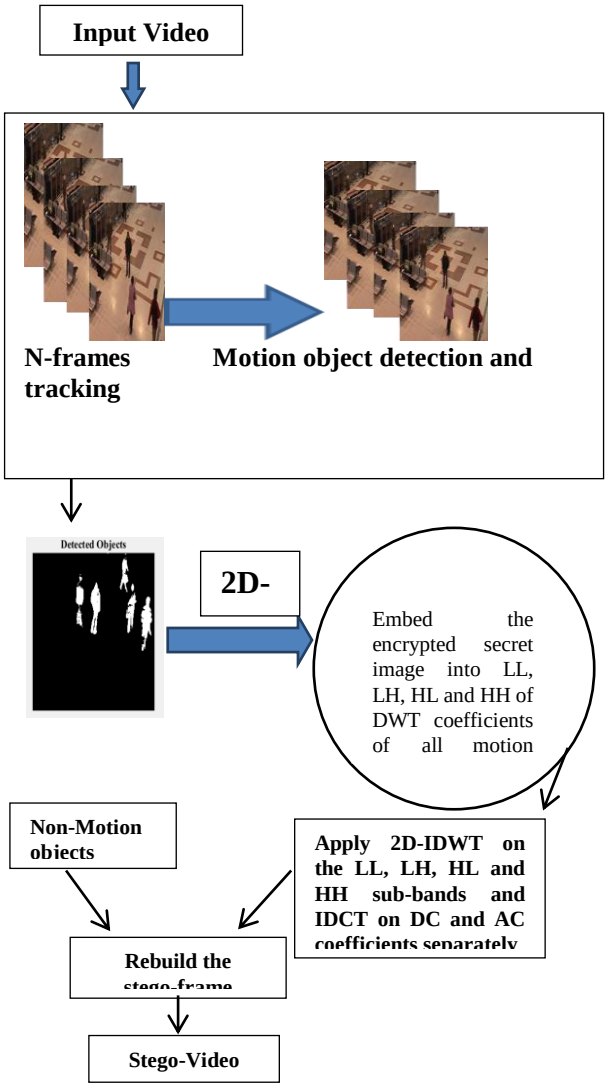


Figure 3. Encoding process of the proposed method

Algorithm-1

Inputs: Cover video, Secret Image

Output: Stego Video

Steps:

1. Video is divided into 'N' frames
2. Identify the moving objects in the video frame
3. Identify the foreground mask of each motion region by computing the differences between consecutive frames.
4. Applying 2D-DWT separately on each motion object for RGB frame components. In addition, 2D-DCT is also applied on the same motion region generating the DC and AC coefficients separately.
5. Apply the step 4 for secret image
6. Conceal the encoded secret image coefficient into the coefficient of R, G and B for each motion object based on its foreground mask.
7. Apply 2D-IDCT and 2D-IDWT separately on each component coefficients to produce the stego frame.
8. Stego frames are rebuild in order to construct the stego video

In order to recover hidden messages accurately, the stego video is separated into a 'N' number of frames. The sequence of data extraction Algorithm-2 is detailed further,

Algorithm-2

Inputs: Stego video

Output: Secret image

Steps:

1. Stego video is divided into 'N' frames
2. Identify the moving objects in the stego video frame
3. Identify the foreground mask of each motion region by computing the differences between consecutive frames.
4. Applying 2D-DWT separately on each motion object for RGB stego frame components. In addition, 2D-DCT is also applied on the same motion region generating the DC and AC coefficients separately.
5. Recover the secret imagefrom the coefficients of R, G and B for each motion object.
6. Apply 2D-IDCT and 2D-IDWT separately on each component coefficients to produce the stego frame.
7. Decoded secret image coefficient into the coefficient of R, G and B for each motion object based on its foreground mask.

IV. RESULT AND ANALYSIS

The results of the proposed algorithm are computed using MATLAB. The following parameters are used to measure the performance: PSNR, MSE, CORRELATION, SSIM and HR.

The cover video consists of a 256 x 256 video dimension at 15 frames/second,with a data rate of 23592 kbps.

Mean Square Error (MSE) is used to measure distortion rate in the received stego-image as per Equation 1 and Peak Signal to Noise Ratio (PSNR) is used to measure the embedding quality of stego-image in dB using Equation 2.

$$MSE = \sum_{x=1,y=1}^{p,q} (Pix_{BEx} - Pix_{AEx})(Pix_{BEy} - Pix_{AEy})/(p*q) \quad (1)$$

Where,

Pix_{AE} = Pixel values after image embedding; Pix_{BE} = Pixel values before embedding

$p * q$ = Image size

$$PSNR = 10\log_{10}(2^Q - 1/MSE) \quad (2)$$

Where,Q = 2# bits per pixel -1

The Hiding Ratio is calculated using Equation 4.

$$HR = \frac{\text{size of embedding image}}{\text{Cover video size}} \times 100 \quad (4)$$

The five test images that are considered to conceal in the cover videos of Fig. 5. in the proposed system are displayed in the Fig. 4.

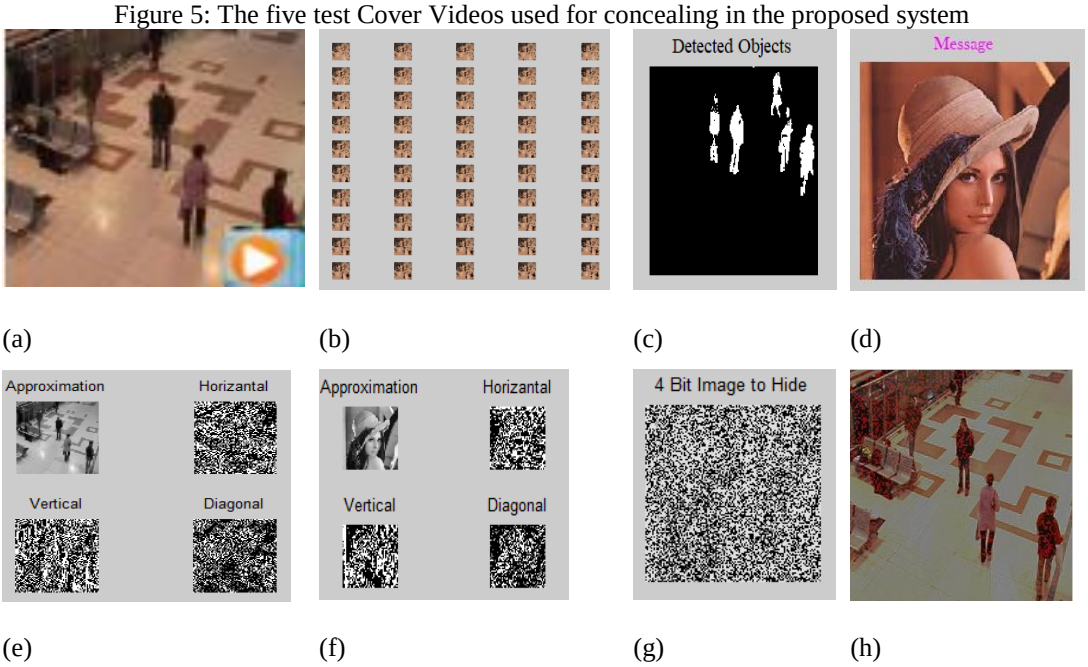
An illustration of embedding is considered to hide the Lena secret image (Figure 4 (d)) in to a cover video 1 (Figure 5(a)) and the sequence of embedding process is displayed in Fig.6.

(a) Vegetable (b) Mandrill (c) Pepper colors (d) Lena (e) Football

Figure 4: The five test Secrete Images concealed in the proposed system

(a) Video 1 (b) Video 2 (c) Video 3 (d) Video 4 (e) Video 5

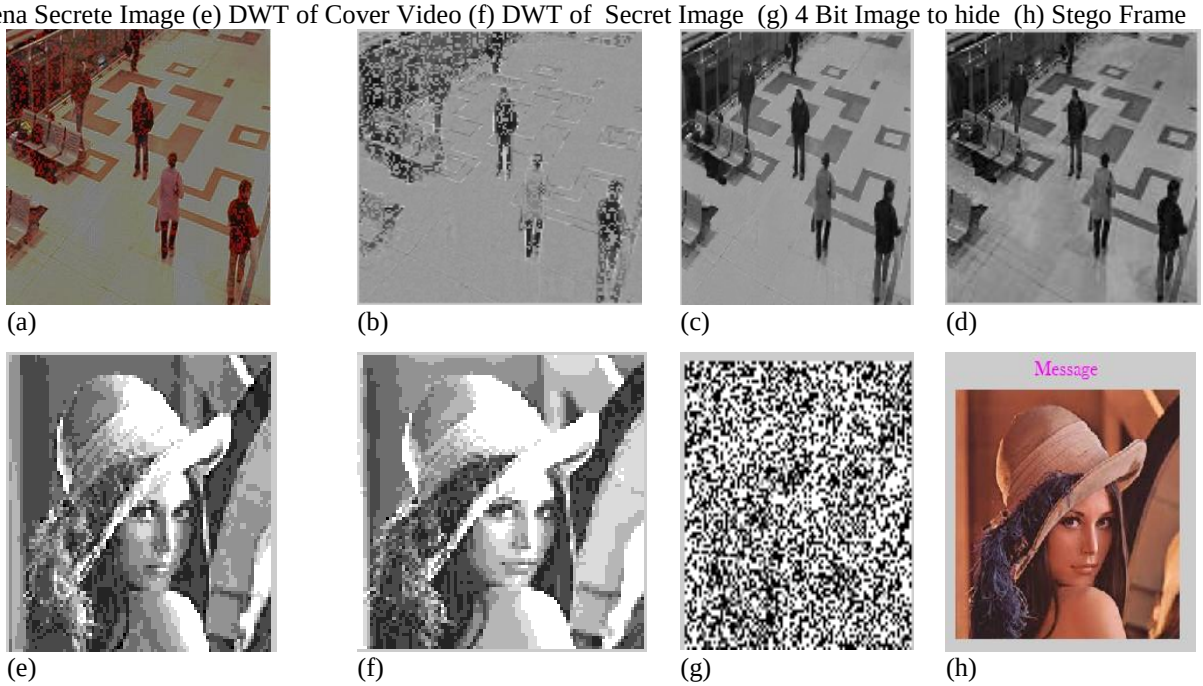
Figure 5: The five test Cover Videos used for concealing in the proposed system



(a) (b) (c) (d)

(e) (f) (g) (h)

Figure 6: Embedding process (a) Cover video (b) Extraction of 'N' frames from Cover Video (c) Object tracking and Detection (d) Lena Secrete Image (e) DWT of Cover Video (f) DWT of Secret Image (g) 4 Bit Image to hide (h) Stego Frame



(a) (b) (c) (d)

(e) (f) (g) (h)

Figure 7: Extraction process (a) Stego video frame (b) IDWT of Red Channel Cover Video frame (c) IDWT of Blue Channel Cover Video frame (d) IDWT Image of Green Channel Cover Video frame (d) Red channel of secret image extracted (e) Blue channel of secret image extracted (f) Green channel of secret image extracted (e) Secrete Image.

The selected cover is discretised in to 'N' number of frames over which detection and tracking is done for motion region so as to identify the foreground mask. Further 2D-DCT and 2D-DWT is implemented on both cover frame and secret image of RGB components. The secret image is concealed using H.264 encoding algorithm to obtain the stego frame. 2D-IDCT and 2D-IDWT is applied on each stego frame to obtain the stego video. Then reverse embedding process is carried out at the destination to retrieve the secret image as shown in Fig. 7.

The performance analysis parameter such as PSNR, MSE, and Correlation for the proposed method is tabulated in Table 1 for five secret images that are concealed in three different test videos. The average PSNR value in dB is computed to be 35.1074with percentage mean square error of 10.142.The three different types of noise attacks such as Gaussian white, Salt & pepper and Speckle are considered to study the influence on the performance parameters of PSNR, MSE,and Correlation is tabulated in Table 2. It is observed that there is negligible effect of the noise attacks on the performance parameters thus proving the robustness of the proposed technique. It is found that the proposed method is better when compared with the existing methods and the values are displayed in Table 3.

Table 1: Proposed System Performance Analysis

Sl. No.	Cover Video	Secret Image	Secret Image size	PSNR	MSE	Correlation
1	Video-1	Lena	512 x 512	34.9226	0.0904	0.8074
		Mandrill	256 x 256	34.8176	0.1063	0.7857
		Pepper	128 x 128	33.9659	0.1027	0.7607
		Vegetable	100 x 100	35.4258	0.0292	0.8252
		Football	80 x 8 0	35.0153	0.0807	0.6561
2	Video-2	Lena	512 x 512	34.9185	0.01038	0.7636
		Mandrill	256 x 256	33.556	0.1129	0.7143
		Pepper	128 x 128	35.0153	0.0807	0.6505
		Vegetable	100 x 100	33.5403	0.1796	0.8182
		Football	80 x 8 0	36.4987	0.2873	0.7352
3	Video-3	Lena	512 x 512	33.9185	0.1038	0.9007
		Mandrill	256 x 256	33.556	0.1129	0.8215
		Pepper	128 x 128	35.1231	0.0807	0.7678
		Vegetable	100 x 100	36.8148	0.0533	0.7978
		Football	80 x 8 0	39.5226	0.0904	0.7814
			Average values	**35.1074**	**0.10142**	**0.7724**

Table 2: Performance analysis of proposed algorithm under various attacks

Type of attack	PSNR	Correlation
No attack	35.4385	0.76477
Gaussian white D=0.5	34.4385	0.80538
Salt and Pepper D=0.5	33.8501	0.80902
Speckle D=0.5	34.0012	0.76716

Table 3: Comparison table of Proposed method with other Existing Methods

Method	PSNR in dB	HR %	DWT/ DCT	H.264 / AVC
Wisam Abed Shukur et al. [16]	29.5	--	YES	NO
Ke et al. [06]	24.54	2.44	NO	YES
Saurabh et al. [17]	34.78	--	NO	YES
Proposed Algorithm (DWT & H.264)	**35.1074**	**4.00**	**YES**	**YES**

V.CONCLUSION

This article presents a new approach whichbinds the idea of video steganography based on transfer domain using DWT and DCT with Multiple Object Tracking as pre-processing stage to provide a improved confidentiality to the secret image preceding the embedding stage using H.264 algorithm. It is observed from the experimentation that the proposed scheme has a average HR of 4.00% with average PSNR of 35.1074 dB and 26% similarity index. It is also observed that the noise attacks have negligible influence on the performance parameters thus proving the robustness of themethod. It is evident from the literature that the proposed method has high embedding capacity, visual quality and robustness& security when compared with existing methods.

REFERENCES

1. Prasad, K. Munivara, V. Jyothsna, S. H. K. Raju, and S. Indraneel, "High Secure Image Steganography in BCBS Using DCTand Fractal Compression", International Journal of Computer Science and Network Security, Vol. 10, No. 4, pp. 162-170, 2010.
2. Xiaojing Ma,Zhitang Li, Hao Tu, and Bochao Zhang, "A Data Hiding Algorithm for H.264/AVC Video Streams Without Intra-Frame Distortion Drift",Ieee Transactions on Circuits and Systems for Video Technology,Vol.20, No. 10, pp.1320-1330, 2010.
3. K.B. Shiva Kumar, K. B. Raja, R. K. Chhotaray, and Sabyasachi Pattnaik, "Performance Comparison Of Robust Steganography Based On Multiple Transformation Techniques", International Journal of Computer Technology Application,Vol. 2, No. 4, pp.1035-1047, 2011.
4. R. Wang, L. Hu, and D. Xu, ''A Watermarking Algorithm Based On The CABAC Entropy Coding For H.264/AVC'', Journalof Computer and Information Systems, Vol. 7, No. 6, pp. 2132–2141, 2011.

5. 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’’,2nd International Conference on Computer and Knowledge Engineering (ICCKE), Vol. 2, pp. 194–198, 2012,
6. N. Ke and Z. Weidong, ‘‘A Video Steganography Scheme Based on H.264 Bitstreams Replace’’, 4th IEEE International Conference on Software Engineering and Service Science (ICSESS), Vol. 4, pp. 447–450, 2013.
7. Tew, Yiqi, and KokSheik Wong, "An Overview of Information Hiding in H. 264/AVC Compressed Video", IEEE Transactions on Circuits and Systems for Video Technology, Vol.24, no. 2, pp. 305-319, 2014.
8. Zafar Shahid, Marc Chaumont, and William Puech, "Considering the Reconstruction Loop for Data Hiding of Intra-and Inter-Frames of H. 264/AVC", Signal, Image and Video Processing-Springer, Vol. 7, no. 1, pp. 75-93, 2013.
9. N.Sathisha, K. R. Venugopal, K. Suresh Babu, K. B. Raja, and L. M. Patnaik, "Non Embedding Steganography Using Average Technique in Transform Domain", Signal Processing and its Applications (CSPA),IEEE 9th International Colloquium, pp. 1-6, 2013.
10. Yunxia Liu, Zhitang Li, Xiaojing Ma, and Jian Liu , "A Robust Data Hiding Algorithm For H. 264/AVC Video Streams", Journal of Systems and Software, Vol. 86, No. 8, pp. 2174-2183, 2013.
11. T. Samitha, C. R. Prasanth, P. R. Lekshmi, and K. P. Shanti, "Study of H. 264/AVC Algorithm and It’s Implementation in MATLAB",IOSR Journal of VLSI and Signal Processing (IOSR-JVSP), Vol. 4, Issue 1, Ver. II, pp. 53-68, 2014.
12. Al-Jammas, Mohammed H., and Noor N. Hamdoon, "AReal-Time H. 264/AVC Encoder&Decoder With Vertical Mode For Intra Frame And Three Step Search Algorithm For Pframe",2ndInternational Conference on Computational Science and Engineering,DOI: 10.5121/csit.2014.4404, pp. 33–44, 2014.
13. Ramadhan J.Mstafaand Khaled M. Elleithy, "A Novel Video Steganography Algorithm in DCT Domain Based on Hamming and BCH Codes",37th IEEE Sarnoff Symposium, pp. 208-213, 2016.
14. Ramadhan J.Mstafa and Khaled M. Elleithy, "Compressed and Raw Video Steganography Techniques: A Comprehensive Survey and Analysis", Multimedia Tools and Applications, Vol. 76, no. 20, pp. 21749-21786, 2017.
15. Ramadhan J.Mstafa,Khaled M. Elleithy, and Eman Abdelfattah, "A Robust and Secure Video Steganography Method in DWT-DCT Domains Based on Multiple Object Tracking and ECC" , IEEE Access, Vol. 5, pp. 5354-5365, 2017.
16. Wisam AbedShukur, Wathiq Najah Abdullah, and Luheb Kareem Qurban, "Information Hiding in Digital Video Using DCT, DWT and CVT", Journal of Physics: Conference Series, Wisam Abed, Vol. 1003, No. 1, pp. 012035. IOP Publishing, 2018.
17. Saurabh Anand and Anand Singh Jalal, “An Efficient Steganographic Approach for H.264/AVC Compressed Videos”, International Journal of Engineering Research in Computer Science and Engineering, Vol 5, Issue 2, pp.1-19, 2018.