Adaptive Algorithm for Watermark Hiding in Video Objects

[1]Prof. Dr. Israa Hadi Ali, [2]Safa S. AL-Murieb
[1]*IT College - Babylon University - Iraq, israa_hadi1968@yahoo.com*
[2]*Ph.D. postgraduate - IT college - Babylon University - Iraq, safasaad1981@yahoo.com*

Abstract

In order to protect and secure a video, watermark is added within data of video, to avoid conceal the watermark in fixed location or in the background of the frames of video, this paper indicates watermark concealing algorithm based on selecting two specific objects that are characterized with activity in their motion over the frames of video file. In this paper the watermark is concealed in objects of video based on host and reference objects, with the variation number of concealed bits in any pixel of object according to the proposed hiding schema that is explained in this paper instead of hiding the same number of bits from watermark. Also, in this work we illustrate the algorithm of watermark hiding in one frame, and we can extend this work by applying this algorithm in each frame based on the host and reference objects.

Keywords: *Information Hiding, Video Object, Watermarking, LSB.*

1. Introduction

In communications ways when the sender sends his/her information to other parity, it may be stolen or modified, so that it needs a protection and security way in order to ensure preservation of original information. To secure the data of multimedia which is in digital form, information is added within it; multimedia can be image, video, audio, or text [1].

There are many methods of data securing and protecting such as cryptography, watermarking, and steganography. Each one has its characteristics and appropriate applications in wide range of data transitions [2]. Whereas a method of converting the source data to another form which is non-readable if the foreign user gets it, except the authorized receiver user can transform it to the original form and can reads it, this protection schema is called cryptography [2][3]. Another different preserving way is by conceal certain information which is in a digital form as text or picture to preserve the absentee of information, this is named as watermarking [3][4], while a schema of writing a data such as any digital signal (audio file, image, text, and video) in another signal that is called a cover, named as steganography [5].

2. Related Works

Many methods and techniques were applied for embedding a watermark in a cover, whereas Al-Taweel [6] based the Hartung technique for video protection from copyright, it was based on spread spectrum in discrete cosine transform (DCT). Agarwal [7] produced video protection method from copyright, firstly DWT was applied, then applying DCT on the (LH and HL) bands of WT, whereas a low frequency coefficients of the watermark was concealed in the coefficients of DCT with midfrequency.

Mostafa [8], Sinha [9], Patil [10], and Chimanna [11] introduced hybrid method of video watermarking, the performance of watermarking was improves by combining two transforms PCA and DWT, in the first step DWT was applied to each frame, then PCA was applied to bands LL and HH, where the watermark was embedded in the result of PCA.

Ahmed [12] hided in frames of video text and gray images information which were encrypted using RSA method, the concealing was applied in the frequency domain, in that work Combined DWT-DCT Algorithm was applied. Tawfiq et al. [13] proposed an intelligent watermark in GIS by combining the watermark with the features that were extracted from the vector map, this gives an intelligent watermark, and hiding the resulted watermark in vector map. Tawfiq et al. [14] proposed a method to hide the message in the highest frequencies segments, these segments were determined by segmenting the image (cover) and clustering them. Tawfiq et al. [15] produced a method to determine blocks of an

image for concealing using QCC that pixels within the block are similar and applying DCT to determine the block of hiding which has large number of zeros.

3. Information Hiding

Due to popularity of internet, communications, and digital media, and unreliability of media, there is necessary for securing and authenticating the data during transmitting it. The process of concealing data is embedding information of authenticity within the original data, with the importance that concealed information isn't perceptual and doesn't influence the nature of perception [16]. The reasons behind hiding or concealing concepts are: preserving the personality and data privacy, there is data that is critical, data's abuse avoidance, preventing data deleting and any modification, and others [3].

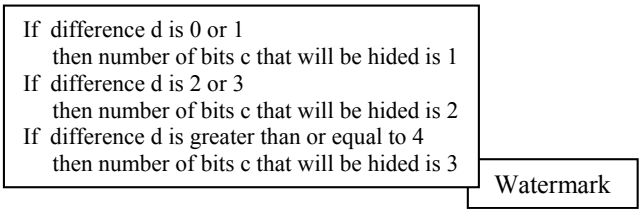
Watermark is preferred to be invisible, it hasn't been seen or percept across the digital multimedia, it is impossible to delete it, this is named robustness, it identifies owner of the data without any ambiguous when retrieving this watermark, the amount of watermark message that will be hidden is called payload or capacity [17]. The main reason of hiding is to protect data from unauthorized use, this includes copy protection (by concealing digital message, it is called watermarking), and to prevent anyone to know about existence of information or message, this is called steganography [18].

Methods of watermarking are applies in two different domains, spatially such as LSB method, or frequently using transformation that convert the digital data form from spatial to frequency domain for example DCT, DFT, and WT, whereas watermarking concealing is applies in the coefficients of the method from these [19]. According to the watermark's perceptual, it can be completely shown, this is visible, such as logo, or it isn't shown (invisible), applications of second type are authentication, copyrighting, and others. According to the watermark's robustness, a watermark is called fragile if it fails to be detected after the simple modification, while a watermark is called semi-fragile, it fails detection after malignant transformations although it resists beginning transformations, and a watermark is to be robust if it withstandsa designated class of transformations [11]. The watermarking systems can be non-blind which means that original cover has been needed in watermark detection operation to guide the position of it in the watermarked cover, this type is also named private watermarking, it can be semi-blind which doesn’t require the original cover but it needs the watermark, or it can be blind which means that both original cover and watermark are not required, it also called public watermarking [20].

4. Proposed Method

The proposed algorithm of watermark concealing in video media is explained in the following block diagram (Figure 1), it indicates the watermark concealing algorithm in frame of video, and it can be expanded for concealing the watermark in many frames.

it describes the hiding in one frame from video frames. The main idea of concealing algorithm is hiding the watermark in the object of video frame, that object has the most motion activity. Instead of hiding fixed number of bits in the Least Significant Bit (LSB) of each pixel of host object, this algorithm is adapted by hiding modified number of bits that will be hidden in the pixels of host object. The adeptness of embedding algorithm is done by determining the number of bits from the watermark that will be hidden according to the difference between the intensity value of the current pixel in host object and its 8-neighbors which surround it. Then calculate the average value of the 8-neighbored pixels of the current pixel of host object (except the pixels in the border of the selected area of an object, the pixels in corners have 3-neighbors and the rest pixels of border have 5-neighbors). After find the difference d between the current pixel and the average of its 8-neighbors, according to this difference, the number of bits *c* from the watermark that will be concealed are determined as follow.



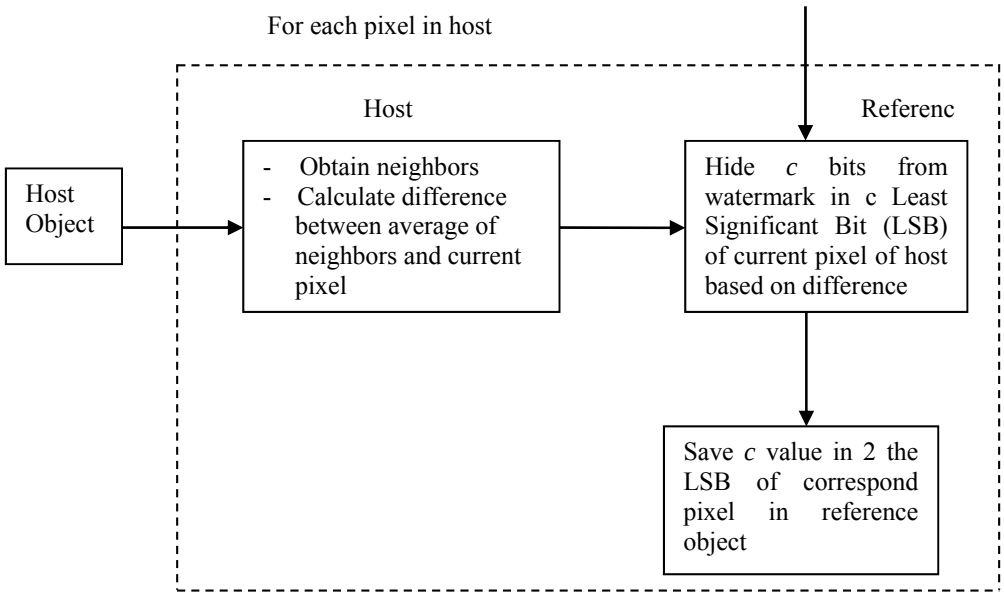


Figure 1. Block diagram of watermark hiding.

This algorithm depends on two active objects (this will be noted in details in the next paper based on tracking all the objects in video). The first most active object is host object and the other is reference object. The number of hided bits *c* in each pixel will be saved in the 2 LSB part of its corresponding pixel in reference object. In the watermark extracting operation and in order to know how many bits were hided in each pixel of host object, the 2LSB of each corresponding pixel of reference object will be checked, this guides in finding the hidden bits of watermark within the host object to extract the watermark from the each frame of video. In this proposed concealing method, watermark is embedding in object of video instead of embedding it in the background or stable position in the frame. The following algorithm describes hiding algorithm.

Algorithm for Watermark Concealing.
Input: Video file and 2D-watermark.
Output: Watermarked video.
Begin
Step 1: Separate video file to set of frames.
Step 2: Convert the watermark into binary form, which is a set of bits.
Step 3: Select two specific objects based on tracking their motion, they are more active in their motion, the first most active object is host object and the other is reference object.
Step 4: For each frame apply the following steps:
Step 4-1: For each pixel in host object do steps (4-2 to 4-6).
Step 4-2: Obtain the 8-neighbors of the current pixel that surround it.
Step 4-3: Calculate the difference *d* between average of 8-neighbors and current pixel using $d=abs(av - p)$ where *av* is average of 8-neighbors of current pixel, and *p* is the current pixel.
Step 4-4: According to the difference *d* that is calculated in previous step, number of bits, *c*, from watermark that will be hidden in the Least Significant Bit (LSB) part of current pixel *P* in host object, is determined as follow:
If d = 0 or 1 then c is 1
If d = 2 or 3 then c is 2
If d >= 4 then c is 3
Step 4-5: Hide *c* bits from watermark in Least Significant Bit (LSB) of host object.
Step 4-6: Store number *c* in the 2bits of the LSB of reference object.
Step 5: Store the size of watermark in the first two bytes in the current frame.
End

The following Figure 2 shows the location for saving the counter number *c* in the 2LSB of corresponding pixel of reference object. This number will be used in extracting the watermark from the host object of each frame of watermarked video to determine the number of embedded bits in each pixel.

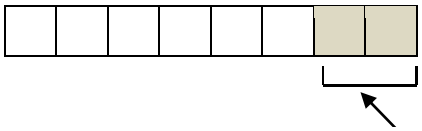


Figure 2. Count representation in corresponding pixel of reference object.

If the arrays that are represent both host and reference objects as shown in the below figure:

53	61	70	55
71	76	87	78
79	78	85	54

Host Object

140	153	170	157
148	157	174	153
163	184	179	172

Reference Object

Figure 3. Example of host and reference objects values.

Now for each pixel in host object obtainits neighbors, such as the neighbors of the first pixel value 53 are three they are 61, 76, 71, then calculate the difference *d* between 53 and average of neighbors. This means that *d*=*abs*(((61+76+71)/3)-53)=16, it is greater than 4, so that number of bits, *c*, of watermark that will be hidden in the LSB part of pixel 53 is three bits, that is represented in binary with two ones in the LSB.

The following figure shows the modification in pixel value of host object and its corresponding pixel in reference object after hiding three bits from watermark in host object and saving the number of hidden bits in the 2LSB of reference object if the watermark after converting it into binary as 1101010101110001.

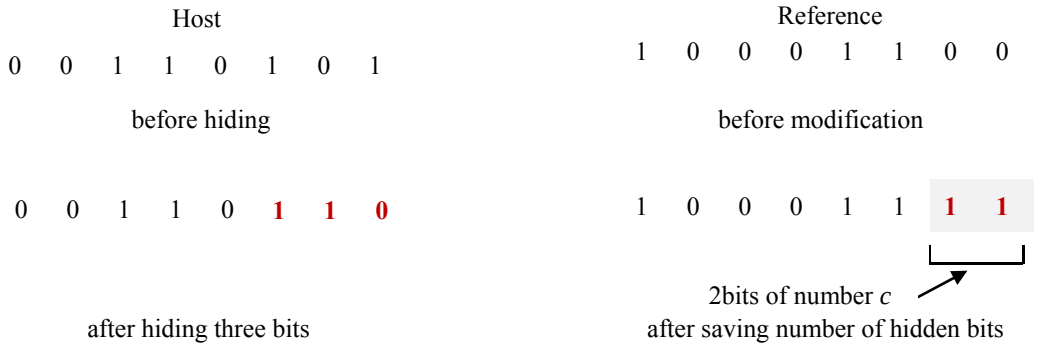


Figure 4. The bits of pixel of host and reference objects before and after hiding.

Now the new value of pixel 53 in host object is 54, and the new value of the corresponding pixel 140 in reference object is 143.

Another explanation for example pixel 76 in the second row and second column, *d*=*abs*(((53+61+70+87+85+78+79+71)/8)-76)=3. So that number of bits, *c*, of watermark that will be hidden in the LSB part of pixel 76 is two bits whereas the binary representation of 76 is 01001100. It will become after hiding two bits of watermark 1101010101110001 as 01001110 that represents value

78, and the binary representation of its corresponding pixel 157 in reference object is 10011101, it will become after saving number of hidden bits as 10011110 that represents value 158.

To extract the embedded watermark, checking the two LSB of each pixels of reference object, and based on the contents of these two bit the number of bits of watermark that were hidden in the corresponding pixel in the host object, are known, as the following:

If the value of 2LSB of the current pixel of reference object is 1
Then get one bit-LSB from the corresponding pixel of host object
If the value of 2LSB of the current pixel of reference object is 2
Then get two bit-LSB from the corresponding pixel of host object
If the value of 2LSB of the current pixel of reference object is 3
Then get three bit-LSB from the corresponding pixel of host object

By iterated this process to the all pixels of reference object, the bits of embedded watermark are grouped and finally retrieving the watermark. The following figure explains the watermark retrieving.

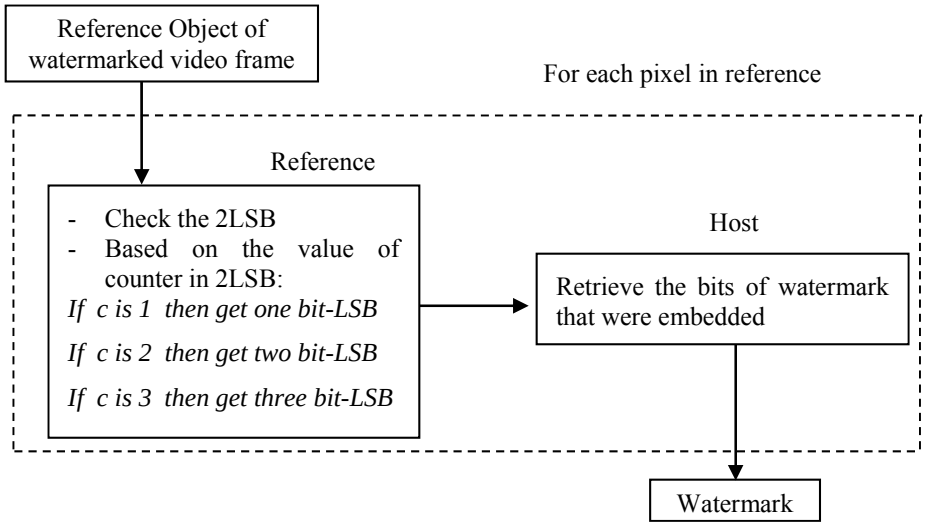


Figure 5. Block diagram of watermark extracting.

The following algorithm explains the watermark extraction.

Algorithm for Watermark Extraction.
Input: Watermarked Video file.
Output: Extracted Watermarked.
Begin
Step 1: Separate watermarked video file to set of frames.
Step 2: Select two specific objects based on tracking their motion, they are more active in their motion, the first most active object is host object and the other is reference object.
Step 3: For each frame apply the following steps:
Step 3-1: For each pixel in reference object do steps (3-2 to 3-5).
Step 3-2: Check the 2LSB of current pixel that represents the counter *c*.
Step 3-3: According to the value of counter *c* that is calculated in previous step the number of embedded bits will be known.
Step 3-4: Get *c* bits from the LSB part of the corresponding pixel of host object to the current pixel of reference object as follow:
If *c* is 1then get one bit-LSB
If *c* is 2 then get two bit-LSB
If *c* is 3 then get three bit-LSB
Step 3-5: Save the bits that are get for building the watermark.
Step 4: Return the extracted watermark.
End

5. Experimental Results

Firstly separate the input video into set of frames, and convert the watermark (it can be image or text) into set of bits, the embedding algorithm was applied into frames of video, the area of embedding in host must equivalent to the area of embedding in reference, with storing the number of pixels of watermark that were hidden in the first two bytes of a frame.

By using many different size of area with different size of the 2D-watermark (watermark image), the PSNR measure was calculated for each frame to determine the amount of modification in both object and reference objects due to the watermark concealing in pixels of host object and the concealing of number of embedded bits from watermark in the corresponding pixel of reference object.

Table 1 explains the experimental results of frame 1 with calculating the PSNR measure of host and reference objects. Table 2 shows the PSNR measure of host and reference objects in frame 2, and so on calculating the PSNR measure of host and reference objects in each frame. Table 3 shows the PSNR measure of host and reference objects in frame 7.

Table 1. The PSNR measure of host and reference objects in frame 1.

Size of host object	Size of reference object	Size of 2D watermark	PSNR of host object	PSNR of reference object	Used pixels for hiding
50*20	50*20	8*5	46.49	52.40	113
40*50	40*50	20*15	41.37	46.24	957
60*30	60*30	11*9	46.57	50.33	294
30*70	30*70	7*10	49.29	52.52	301
80*100	80*100	20*10	49.46	53.78	628
90*110	90*110	20*30	45.73	49.96	1846

Table 2. The PSNR measure of host and reference objects in frame 2.

Size of host object	Size of reference object	Size of 2D watermark	PSNR of host object	PSNR of reference object	Used pixels for hiding
50*20	50*20	8*5	46.33	51.58	116
40*50	40*50	20*15	42.28	45.16	980
60*30	60*30	11*9	48.44	50.25	286
30*70	30*70	7*10	48.13	52.47	297
80*100	80*100	20*10	49.41	51.82	611
90*110	90*110	20*30	46.84	50.79	1827

Table 3. The PSNR measure of host and reference objects in frame 7.

Size of host object	Size of reference object	Size of 2D watermark	PSNR of host object	PSNR of reference object	Used pixels for hiding
50*20	50*20	8*5	47.02	54.24	105
40*50	40*50	20*15	43.11	48.21	926
60*30	60*30	11*9	45.86	52.41	295
30*70	30*70	7*10	49.73	53.12	292
80*100	80*100	20*10	47.58	51.53	674
90*110	90*110	20*30	44.87	48.98	1873

Table 4 explains the PSNR such as of entire frame 5 that includes unchanged areas (any area in a frame except that of more two active objects), and changed areas (where the watermark was been hide in host object, and number of bits that were hidden in each corresponded pixel in reference object.

Table 4. The PSNR measure of entire frame 5.

Size of host object	Size of reference object	Size of 2D watermark	PSNR of frame 5
50*20	50*20	8*5	68.13
40*50	40*50	20*15	65.74
60*30	60*30	11*9	62.79
30*70	30*70	7*10	63.38
80*100	80*100	20*10	56.96
90*110	90*110	20*30	57.19

6. Conclusions

In order to increase the powerful and the characterized hiding algorithm of this paper, it doesn't depend on hiding the watermark in fixed place in the frames of video.

To avoid the weakness of watermark concealing in the same place through the video frames, so that the adaptive algorithm of this paper tends to conceal the watermark in different locations within the frames depending on selecting two objects (host and reference) which are active in their motion through the video, whereas the location of hiding watermark varied according to the motion of these objects.

Also this algorithm doesn't conceal fixed number of bits from watermark in LSB part of each pixel, instead of that, in each time the algorithm conceals varied number of bits from watermark in LSB part of each pixel of host object depending on the difference between the current pixel and its neighbors, with storing the number of hidden bits in 2LSB of reference object.

The experimental results show a small modification in both object and reference objects, which is determined by PSNR measure, this doesn't cause perceptual degradation in frames of video duo to the hiding operation using LSB, many pixels in the area of host and reference objects are modified, whereas LSB modifies as maximum 3bits in the least significant part of the pixel. So that only area of hiding in both objects are changed in its pixels values (not all its pixels, just they are enough for hiding watermark bits).

7. References

[1] Komal Patel, Sumit Utareja, Hitesh Gupta, "A Survey of Information Hiding Techniques", International Journal of Emerging Technology and Advanced Engineering, vol.3, Issue 1, pp.347-350, 2013.
[2] Richa Gupta, "Information Hiding and Attacks : Review", International Journal of Computer Trends and Technology (IJCTT), vol.10, no.1, pp.21-24, 2014.
[3] Richa Gupta, Sunny Gupta, Anuradha Singhal, "Importance and Techniques of Information Hiding : A Review", International Journal of Computer Trends and Technology (IJCTT), vol.9, no.5, pp.260-265, 2014.
[4] Sourav Bhattacharya, T. Chattopadhyay and Arpan Pal, "A Survey on Different Video Watermarking Techniques and Comparative Analysis with Reference to H.264/AVC", In Proceedings of the IEEE International Symposium on Consumer Electronics, pp.1–6, 2006.
[5] Fabien A. P. Petitcolas, Ross J. Anderson, Markus G. Kuhn, "Information Hiding: A Survey", Proceedings of the IEEE special issue on protection of multimedia content, pp.1062-1078, 1999.
[6] Sadik Ali M. Al-Taweel, Putra Sumari, Saleh Ali K. Alomari, Anas J. A. Husain, "Digital Video Watermarking in the Discrete Cosine Transform Domain", Journal of Computer Science, vol.5, Issue 8, pp.536-543, 2009.
[7] Aditi Agarwal, Ruchika Bhadana, Satishkumar Chavan, "A Robust Video Watermarking Scheme using DWT and DCT", (IJCSIT) International Journal of Computer Science and Information Technologies, vol.2, Issue 4, pp.1711-1716, 2011.
[8] Salwa A.K Mostafa, A. S. Tolba , F. M. Abdelkader, Hisham M. Elhindy, " Video Watermarking Scheme Based on Principal Component Analysis and Wavelet Transform", IJCSNS International Journal of Computer Science and Network Security, vol.9, no.8, pp.45-52, 2009.
[9] Sanjana Sinha, Prajnat Bardhan, Swarnali Pramanick, Ankul Jagatramka, Dipak K. Kole, Aruna Chakraborty, "Digital Video Watermarking using Discrete WaveletTransform and Principal Component Analysis", International Journal of Wisdom Based Computing, vol.1, Issue 2, pp.7-12, 2011.
[10] Supriya A. Patil, Navin Srivastava, "Digital Video Watermarking Using Dwt And Pca", IOSR Journal of Engineering (IOSRJEN), vol.3, Issue 11, PP.45-49, 2013.
[11] Mohan A Chimanna, S. R. Khot, "Digital Video Watermarking Techniques for Secure Multimedia Creation and Delivery", International Journal of Engineering Research and Applications (IJERA), vol.3, Issue 2, pp.839-844, 2013.
[12] Eman A. E. Ahmed, Hassan H. Soliman, Hossam E. Mostafa, "Information Hiding in Video Files Using Frequency Domain", International Journal of Science and Research (IJSR), vol.3, Issue 6, pp.2431- 2437, 2014.
[13] Tawfiq A. Abbas, Majid J. Jawad, "Proposed an Intelligent Watermarking in GIS Environment", Journal of Earth Science Research, vol.1, Issue 1, PP.1-5, 2013.
[14] Tawfiq A. AL-Asadi, Ali Abdul Azzez Mohammed Baker, "A Novel Method for Image Steganography Based on Texture Features", International Multidisciplinary Research Journal European Academic Research, vol.II, Issue 1, pp.193-203, 2014.
[15] Tawfiq A. AL-Asadi, Abdul Kadhem Abdul Kareem Abdul Kadhem, "Determine Blocks of Image for Hiding Operation Based on Quad Chain Code and DCT", International Multidisciplinary Research Journal European Academic Research, vol.II, Issue 10, pp.12678-12689, 2015.
[16] Arup Kumar Bhaumik, Minkyu Choi, Rosslin J.Robles, and Maricel O.Balitanas , "Data Hiding in Video", International Journal of Database Theory and Application, vol.2, no.2, pp.9-16, 2009.
[17] T. JAYAMALAR, Dr. V. RADHA, "Survey on Digital Video WatermarkingTechniques and Attacks on Watermarks", International Journal of Engineering Science and Technology, vol.2, Issue 12, pp.6963-6967, 2010.
[18] Pallavi N. Holey, Ajay P.Thakare, Harsha R. Vyawahare, "A Secure Data Hiding in Video: A Review", International Journal of Current Engineering and Technology, vol.4, no.6, pp.3951-3953, 2014.
[19] Mahima Jacob, Saurabh Mitra, "Video Watermarking Techniques: A Review", International Journal of Recent Technology and Engineering (IJRTE), vol.4 , Issue 2, pp.1-4, 2015.

[20] Hyung-suk Chu, Ariunzaya Batgerel, Chong-Koo An, "A Semi-blind Digital Watermarking Scheme Based on the Triplet of Significant Wavelet Coefficients", Journal of Electrical Engineering & Technology, vol. 4, no.4, pp.552-558, 2009.