❏      3332

# Robust Video Watermarking Scheme Based on Intra-Coding Process in MPEG-2 Style

**Rakesh Ahuja[1], S. S. Bedi[2]**
[1]Departement of Computer Science & Engineering, Moradabad Institute of Technology, Moradabad, India
[2]Dept of Computer Science & Information Technology, MJP Rohilkhand University, Bareilly, India

| Article Info | ABSTRACT |
|---|---|
| | The proposed scheme implemented a semi blind digital watermarking method for video exploiting MPEG-2 standard. The watermark is inserted into selected high frequency coefficients of plain types of discrete cosine transform blocks instead of edge and texture blocks during intra coding process. The selection is essential because the error in such type of blocks is less sensitive to human eyes as compared to other categories of blocks. Therefore, the perceptibility of watermarked video does not degraded sharply. Visual quality is also maintained as motion vectors used for generating the motion compensated images are untouched during the entire watermarking process. Experimental results revealed that the scheme is not only robust to re-compression attack, spatial synchronization attacks like cropping, rotation but also strong to temporal synchronization attacks like frame inserting, deleting, swapping and averaging. The superiority of the anticipated method is obtaining the best sturdiness results contrast to the recently delivered schemes.<br><br> |

***Corresponding Author:***

Rakesh Ahuja,
Departement of Computer Science & Engineering,
Moradabad Institute of Technoilogy,
Ram Ganga Vihar, Phase 2, Moradabad, Uttar Pradesh, India.
Email: ahuja2305@gmail.com

## 1.    INTRODUCTION

The rapid development of fast internet bandwidth, excellences recording devices, tremendous storage capacity, better noise resistance and quality of services (QoS) have made possible to generate the multiple copies of the digital multimedia content like image, audio and video for distributing to other user or computer system with no quality degradation as the original and copied data are exactly same, inexpensive and delivery to the remote workstation is almost instantaneous.  Therefore, an issue of intellectual copyright protection becomes a major concern. The technology of cryptography solves the problem up to some extent. Howe   ver, the technology vulnerable once the contents are decrypted since a pirate could easily purchase a copy and then re-sell or distribute it over a shared network.  The advent of digital watermarking technology conquers the restriction in presence of some existing threads. Digital watermarking [1] is the process of inserting the special bit pattern as digital watermark into the multimedia document in such that the quality of video must not be degraded from the minimum threshold and it must withstand normal processing of video editing operation. The watermark may be the copyright logo, owner, distributor or customer information, depends upon the application for which it is to be developed.

An exhaustive research has already been take place for image watermarking. The image watermarking techniques [2]-[3] are applied to video multimedia objects too. However, these schemes always suffer because video consisting additional features that do not present in the image. The distinguishable feature of video is the presence of temporal redundancies exists between neighboring frames

unlike image. The robust and imperceptible video watermarking is perpetuity differing from image watermarking. Accustomed video watermarking method [4] suggested decompressing the video stream into typical video, insert the watermark and encode the watermarked video. This procedure requires a enormous processing time to decompress, embed and recompress the video objects. In order to make the system faster and more practical, it is suggested to embed the copyright information during the compression. The practical benefit associated with this scheme is that it supports real time video watermarking applications where embedding process runs parallel with compression, for example, video on demand.

Zho Zhongjie et al. [5] proposed the video watermarking scheme based on motion vectors. The technique utilized the P-frames and B-frames for embedding purpose. The watermark capacity is different in each frame. The dilemma associated in this process is the less payload capacity of watermark information is allowed because such frames are highly compressed by motion compensation procedure. The other issue related with this scheme is the increase in bit rate of macro blocks that were watermarked. Further, the scheme is not robust against frame averaging and frame dropping attack. Another compressed domain based video watermarking scheme is described by Yoshito Ueno [6]. In this technique, the composition of MPEG encoder [7] is partially modifying to embed the watermark information. Two methodologies *Binary Tree* and *Chain Code* are adopted in this scheme. Both techniques utilized the binary watermark as copyright for embedding purpose. A two dimensional watermark is converted into one dimensional array used to pick one bit at a time. In binary tree algorithm, if the picked watermark bit is *1* then the macro block of I-frame referred to motion vector of P-frame is changed to even otherwise odd. In chain code method, macro block of I-frame is partitioned into 8 sections on the origin of the route of motion vectors of P-frame and embed the three watermark bits into one of the 8 parts of macro block of I frame by using octal chain method. A satisfactory perceptibility is obtained however, the scheme lost the watermark bits about 20% while extracting. Robustness is certainly affected sharply when any further video editing operations were applied on watermarked video. MPEG-2 based digital video watermarking scheme is described by Yuk Ying Chung [8] too. The scheme embeds a watermark into the quantized DCT coefficient generated from I-frames during the encoding process. One watermark bit is embedded into the LSB of each DCT coefficient block of I-frames. Watermarking scheme is combined with three error correcting codes: BCH (31,8), Turbo (3,1) and Conv (2,1,3) and found BCH (31,8) achieved higher error correcting capacity than Turbo (3,1) and Conv (2,1,3). Seven cases of noise were simulated and tested. The major drawback associated with this approach that the watermark is distorted or even eliminated by randomizing the LSB of all DCT blocks. Another limitation of this approach is that perceptibility and robustness with respect to frame editing operations were not tested. Ming Jiang et al. [9] described the video watermarking scheme based on MPEG-2 structure for protecting the copyright of the concern multimedia objects. The scheme adopted the simple approach to insert the binary watermark into the host signal. In this technique, I-frames are used to generate the quantized DCT blocks. The embedding algorithm started to pick one watermark bit and one 8x8 DCT block simultaneously and insertion is based on testing the DC value for odd or even. If the watermark bit is odd and the corresponding DC coefficient is also odd then no need to change the DC coefficient otherwise make the DC coefficient to even. Two major drawbacks are associated with these schemes. Minor updating these coefficients degrades the quality of watermarked video sharply as DC coefficient of DCT blocks represent the average information of the video frame directly affect the HVS since these regions are highly sensitive to the HVS and second reason is that watermarking method utilizing such coefficients are responsible for increase in bit rate. The above mentioned techniques inserted the watermark object by exploring the entire DCT blocks from entire or selected I-frames results the degradation of quality of watermarked video and no means of satisfactory level of robustness obtain against temporal synchronization attacks.

The proposed digital video watermarking scheme focused on these limitations by exploiting the features of 8x8 DCT blocks during intra-encoding process considering I-frames in MPEG-2 style. This scheme classifying the DCT blocks in three categories: edge, texture and plain block. Watermark object is embedded into the quantized plain type of DCT blocks. The selection is necessary to avoid degrading the perceptibility of watermarked video from the minimum threshold as these blocks are less sensitive to HVS as compared to other types of blocks. The perceptibility is further improved by employing single AC coefficient from a particular plain DCT block. Another reason for selecting particular type of blocks is to control the increase in bit rate of resultant watermarked video too.

The rest of the paper is organized in the following sections. Section 2 described a concise overview of MPEG-2 video compression standard along with key aspect of suggested video watermarking process. The proposed video watermarking scheme is illustrated in Section 3. The simulation results for robustness and perceptibility issues are elaborate in Section 4. Section 5 contrasts the results of proposed scheme with those techniques published in recent years. Section 6 concludes the work in this paper.

## 2.   MPEG-2 STRUCTURE

The target of development of MPEG-2 algorithm tools is to achieve high compression ratio both in spatial and temporal domain for video multimedia objects. As shown in Figure 1, the structure permits to segment the video into the number of frames.  Three frames are categorized as Intra-picture frames typically called I-frames, forward-predicted frames identified as P-frames and bidirectional frames named as B-frames.

A typical MPEG-2 coding standard [10]  creates a group of sequence of pictures termed as GOP. The structure of GOP consisting one I-frame followed by a chain of P-frame and B-frames. The display order and processing order is different as shown in Figure 2 and Figure 3 respectively proposed by [10] . MPEG-2 does not adamant about the size of GOP. The flexibility is beneficial for compression and watermark technology both. I-frames are encoded to reduce the spatial redundancy therefore no reference from other frames is required. P-frames and B-frames are used to minimize the spatial and temporal redundancy both. P-frames is use to predict from the previous I-frames or P-frames. The blocks associated with P-frames are comparable to the set of block of same size in the previous I-frames or P-frames. The best matching block in the reference frame is used to predict for the latter. B-frames employs two references frames and these two types may be  the combination of I-frames and P-frames or both P-frames. In a classical sequence, encoded I-frame is three times larger than a coded P-frame, which is two times larger than I-frames. Thus the highest compression is provided by B-frames. There are numerous key technologies used in MPEG-2 structure such as DCT, quantization, motion estimation and motion compensation and VLC coding. These are broadly classifying into three major parts: intra-coding process, inter-coding process and encoded bit stream. Previous suggested work exploits one of these areas to implement the video watermarking scheme. Watermarking through inter-coding phase is based on intelligently utilizing the motion vectors used for generating the motion compensated image in alliance of P-frames and B-frames. There are two major problems  associated while embedding the watermark in such frames.  First issue is the holding of less capacity of watermark objects as they are highly compressed by motion estimation based technique. Secondly, the bit-rate of resultant watermarked video increases by exploiting these such frames.  The primary advantage of encoded bit stream based video watermarking is that no encoding and decoding required during the insertion and retrieval process respectively. Yet, a limited information as watermark is allowed to insert the watermark object into the host. Another constraint is the increase in computational complexity.

Desiging the watermarking system through intra-coding process is promising to utilize the DCT and quantization process processed through I-frames. Quantized 8x8 DCT block contains one DC and 63 AC coefficients. DC coefficient based watermarking system suffers from degrading the visual quality of watermarked video as the average information is concentrated in this coefficient. AC coefficients are rich source of high frequencies i.e. contains a very small value. Considering entire AC coefficients degrade the perceptibility significantly therefore exploiting few coefficients not only support the human visual system (HVS) by preserving the visual quality of watermarked object but also control on increase in bit rate. Therefore it is suggested that AC coefficients based watermarking scheme with some constraint not only provides high visual quality of watermarked video but also withstand against temporal synchronization attacks like frame insertion, deletion, swapping and averaging. In view of merit of it, the proposed scheme has chosen such areas for designing the video watermarking system in order to obtain the balance tradeoff between perceptibility and robustness.
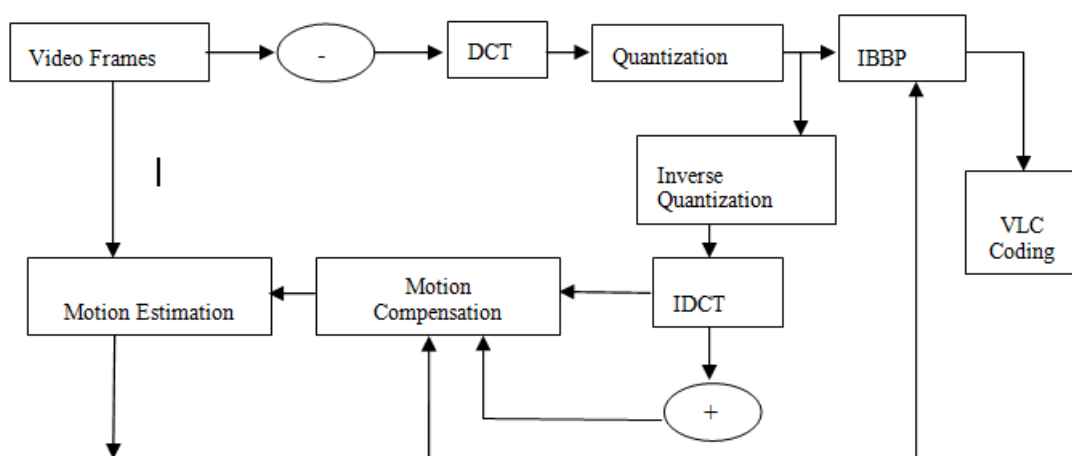


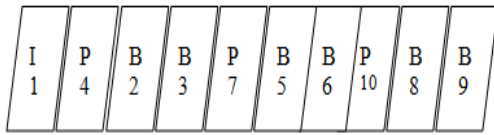Figure 1.  Block diagram of MPEG-2 Structure
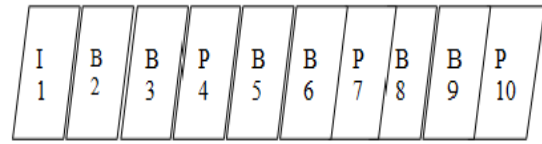
Figure 2.  Decoding and display order of GOP



Figure 3.  Encoding and processing order of GOP

## 3.    PROPOSED METHOD

The  proposed  model  of  video  watermarking  algorithm  is  based  on  encoding  the  raw  video  in MPEG-2 standard. The binary watermark is embedded only in those selected quantized 8x8 DCT blocks which are categorized as plain DCT block as defined in section 3.2. The characteristics of the video frame are analyzed in order to find the appropriate DCT block used to insert one watermark bit and so there is a one to one mapping between inserting bit and selected block. Single coefficient instead of several AC coefficients exploited to obtain the better quality of watermarked video as minimum changes are required during watermarking process.  This not only minimizes the computation cost but also aid to maintain the quality of watermarked video. The embedding process requires only two frequency coefficients lies at rightmost bottom represented by an oval shape as shown in the Figure 4. The simulation results to obtain the elapsed CPU time for watermarking purpose is eloborated in the experimental section 4.3.

### 3.1.  Key generations and watermark preprocessing

A two dimensional binary image *Watermark.tif*  having bit depth *1* used as watermark. Three keys as (K1, K2, K3) are extracted from the watermark itself in the following manner. K1 and K2 denotes the number of rows and columns respectively has been used to extract the watermark. K3 is evaluated from the size of the watermark and treated as third key used to stop the extraction process while recovering the watermark.   A watermark object is encrypted by using double columnar transposition method [11] before inserting into viode object to further enhance the security of the watermark itself. The encrypted object is converted into one dimensional array as $B_w = \{\{W_s\}, s=1, 2,\ldots\ldots N;\ W_s \in \{1, 0\}\}$ to pick one bit at a time.

### 3.2.  Extraction of smooth discrete cosine transform blocks

Discrete cosine transform [12] is the process of splitting the host signal into four frequency bands; DC, low frequency ($L_f$), high frequency ($H_f$) and edges ($E_d$) as shown in following Figure 4. DC characterize the  average  information  contained  by  the  signal.  $L_f$  represents  the  low  frequencies  regions  whereas  $H_f$ expresses the pixels lies on high frequencies regions. Finally, $E_d$ denotes the pixels containing the frequencies at  edge  regions.  DCT  and  further  quantization  operation  reduces  the  spatial  redundancy  by  concentrating energy in few coefficients lies at left upper  part of the block. Each DCT block of 8 x 8 pixels is further classified to recognize the type of DCT block as per the following conditions [13]. A block is treated as edge block if $\left(\left(\frac{\sum L_f + \sum E_d}{\sum H_f}\right) > 4\right)$ otherwise if $(\sum E_d + \sum H_f) \leq 125$ then the block is considered as plain type block and it is classified as texture block if  $\left(\left((\sum L_f + \sum H_f) > 290\right)\right)$. The plain type of blocks are the concern in the proposed scheme as these blocks support HVS and rest others are ignored from watermarking process however always be a part of  MPEG-2 compression process.

| DC(1,1) | $L_f$(1,2) | $L_f$1,3) | $E_d$ (1,4) | $E_d$ (1,5) | $E_d$ (1,6) | $E_d$ (1,7) | $H_f$(1,8) |
|---|---|---|---|---|---|---|---|
| $L_f$(2,1) | $L_f$(2,2) | $E_d$ (2,3) | $H_f$(2,4) | $H_f$(2,5) | $H_f$(2,6) | $H_f$(2,7) | $H_f$(2,8) |
| $L_f$(3,1) | $E_d$ (3,2) | $E_d$ (3,2) | $H_f$(3,4) | $H_f$(3,5) | $H_f$(3,6) | $H_f$(3,7) | $H_f$(3,8) |
| $E_d$(4,1) | $H_f$(4,2) | $H_f$(4,3) | $E_d$ (4,4) | $H_f$(4,5) | $H_f$(4,6) | $H_f$(4,7) | $H_f$(4,8) |
| $E_d$ (5,1) | $H_f$(5,2) | $H_f$(5,3) | $H_f$(5,4) | $H_f$(5,5) | $H_f$(5,6) | $H_f$(5,7) | $H_f$(5,8) |
| $E_d$ (6,1) | $H_f$(6,2) | $H_f$(6,3) | $H_f$(6,4) | $H_f$(6,5) | $H_f$(6,6) | $H_f$(6,7) | $H_f$(6,8) |
| $E_d$ (7,1) | $H_f$(7,2) | $H_f$(7,3) | $H_f$(7,4) | $H_f$(7,5) | $H_f$(7,6) | $H_f$(7,7) | $H_f$(7,8) |
| $H_f$(8,1) | $H_f$(8,2) | $H_f$(8,3) | $H_f$(8,4) | $H_f$(8,5) | $H_f$(8,6) | $H_f$(8,7) | $H_f$(8,8) |

Embedding  region

Figure 4. Classification of 2-D DCT block

### 3.3. Watermark Insertion Process

The embedding method is started with extracting the I-frame from each GOP. The extracted I-frame is further divided into three channels; one as luminance channel $Y$ and other two Chroma channels known as $C_B$ and $C_R$ respectively. Segregate the Y-component, the most luminance part, into non-overlapping 8*8 blocks to apply the DCT and quantization operation using standard quantization matrix. Once it is confirmed that the current block is smooth DCT block then the embedding process of inserting one scrambled watermark bit is delivered as follows:

$$H_f(8,7) = \begin{cases} \text{No change,} & \begin{cases} W_s = 0 \\ (H_f(8,7) < H_f(8,8)) \end{cases} \\ H_f(8,7) - \alpha - \text{threshold,} & \begin{cases} W_s = 0 \\ (H_f(8,7) > H_f(8,8)) \end{cases} \\ \text{No change,} & \begin{cases} W_s = 1 \\ (H_f(8,7) > H_f(8,8)) \end{cases} \\ H_f(8,7) + \alpha + \text{threshold,} & \begin{cases} W_s = 1 \\ (H_f(8,7) > H_f(8,8)) \end{cases} \end{cases} \quad (1)$$

For this purpose, only two AC coefficients are utilized and one of them requires changing marginally as per the clause (1) defined above. To insert another bit, select another quantized plain DCT block to embed just next bit of watermark by using the same method described above. The process is repeated till entire watermark bits inserted in equal number of plain types of blocks. During this process, some plain DCT blocks may be untouched if the numbers of such blocks are larger than the number of watermark bits. In order to reduce the probility of estimating the relationship between watermark bits and DCT blocks, again watermark bits will be started to embed watermark bits from the scratch for remaining such blocks. Although this process consumes unnecessary CPU cyles but provides the additional security to the overall watermarking process.

A threshold must be set by confirming that the lower value must remain lower and higher value must remains higher for those coefficients participating in the watermarking process. The significance of constant $\alpha$ is set to *0.1* ensures that this watermarking algorithm works perfectly even if the threshold is fixed to zero. The threshold best worth obtained at 0.3 evaluated by experimental results explained in section 4.1. The scheme reflects that most of the DCT blocks, comes under the category of edge and texture block remain unchanged during the watermarking. It not only maintains the visual quality of watermarked video but also offer high robustness. The structure of 8th quantized plain DCT block from 131st I-frame before and after embedding the watermark bit *1* is illustrated in Figure 5 and Figure 6 respectively.
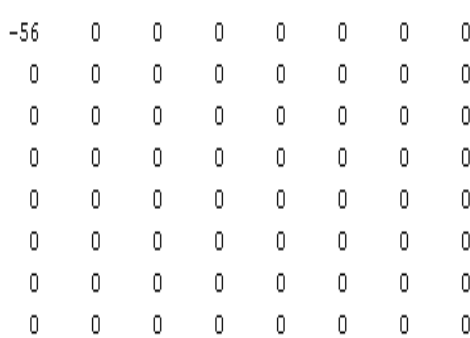
| -56 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

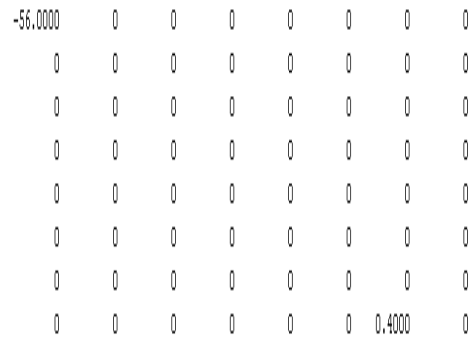| -56.0000 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0.4000 | 0 |

Figure 5. Quantized DCT block          Figure 6. Watermarked Quantized DCT block

### 3.4. Watermark Extraction Process

The estimation of watermark bits is based on the relationship between the coefficients belongs to embedding region. The process of retrieval of watermark object is started by creating the blank matrix with the aid of two keys *K1* and *K2* defined at section III-A. Initialize it by inserting with 'all zeros'. This way ensure about the size of the retrieving watermark. Partition the watermarked video into the sequence of frames. While processing I-frame, convert it into YCBCR spacing. Select the Y component require to

segment into 8x8 non overlapping blocks used to perform DCT followed by quantization process. The extraction process is started just after confirming that the current block is plain DCT block. The retrieval of bits is described as follows:

$$W'_s = \begin{cases} 0, & H_f(8,7) < H_f(8,8) \\ 1, & else \end{cases} \qquad (2)$$

if the coefficient value of $H_f(8,7)$ is less than the coefficient value of $H_f(8,8)$ then watermark bit '0' otherwise '1' is extracted and store into the buffer. Now the buffer is incremented by one. Before incrementing the buffer, one more condition is applied to check that whether the buffer size is equal to the size of third key *K3* defined at section 3.1. If the clause is true then extraction process will stop otherwise continue to extort another quantized plain DCT block to approximate next bit of watermark. However, the recovered watermark is in encrypted form which is decrypted by using the double columnar transposition algorithm [10].

## 4. EXPERIMENTAL RESULTS AND ANALYSIS

The performance of the video watermarking scheme in this paper appraised by accomplishing total 6 standard video sequences as *Akiyo, Foreman, Mother, Hall, Container and Coastguard* with different motion complexity. These video sequences have minimum 300 and maximum 350 frames. The clip *Akiyo* is static video sequence having still background. A newsreader is having only lips movements and rest part of the video including background is immovable throughout the playing of video. *Foreman* sequence is of dynamic motion complexity since a frequent scene change occurs during the entire playing of video clip. *Mother* and *Hall* are almost still background and little foreground motion scene noticed. *Container* is slow background and slow foreground motion scene. *Coastguard* is continuous motion complexity video. A binary watermark *logo.tif* with size 50 x 100 is chosen as shown in the Figure 7b. Sample videos with watermark are explored in Figure 7.
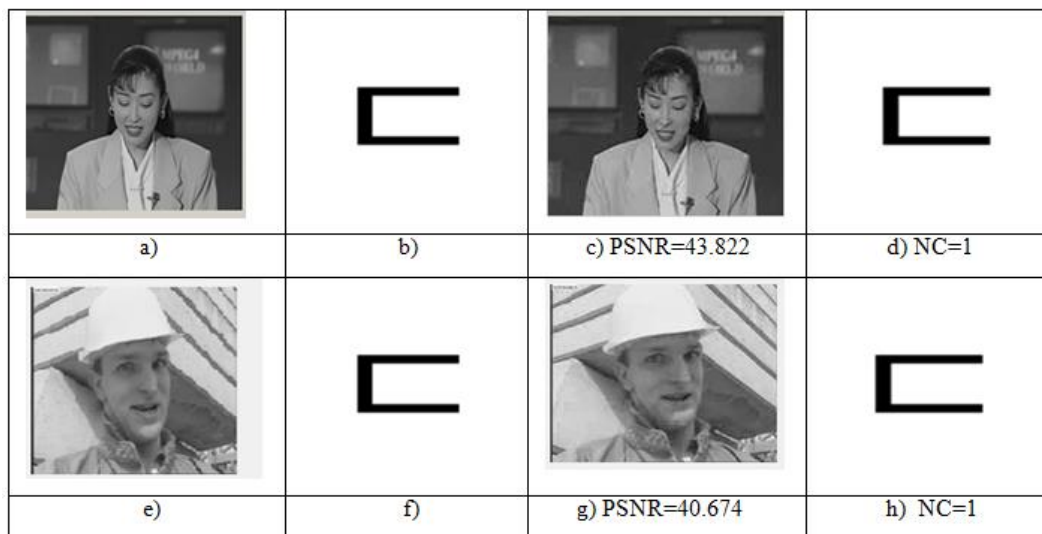


Figure 7. Simulation results from proposed video watermarking Scheme

a) 90th original frame from Original Video *Akiyo*
b) Original Watermark *logo.tif*
c) 90th Watermarked Video frame
d) Extracted watermark
e) 95th raw video frame
f) Pure watermark 'logo.tif' used to insert in raw video sequence Foreman
g) 90th Watermarked video frame from watermarked video sequence Foreman
h) Extracted watermark from watermarked video sequence Foreman with no attacks

The simulation results for evaluating the performance of this algorithm are categorized in three ways: Evaluating the threshold, testing the average perceptual quality and estimating the robustness against intentional, unintentional signal processing, re-encoding and frame based attacks. These measuring parameters are described as follows:

$$PSNR_i = 20\log_{10}\left((\text{Highest}_i)\middle|\sqrt{MSE}\right) \tag{3}$$

$$MSE = \frac{1}{MxN}\sum_{i=1}^{M}\sum_{j=1}^{N}\left[F_{(i,j)} - F_{W_{(i,j)}}\right] \tag{4}$$

$$PSNR_{avg} = \frac{\sum PSNR_i}{n} \tag{5}$$

The perceptual quality of watermarked video is determined in terms of Peak Signal To Noise Ratio ($PSNR_i$) where *i* denotes the ith watermarked video. $PSNR_{avg}$ is obtained by summing the PSNR from all the watermarked sequences divided by the total number of video sequences (n). The robustness is evaluated by the following method.

$$NC = \frac{\sum_i\sum_j W(i,j).W'(i,j)}{\sum_i\sum_j[W(i,j)]^2} \tag{6}$$

$W(i,j)$ and $W'(i,j)$ are the pixels of original and extracted watermarks respectively.

### 4.1. Threshold Setting

Six standard video sequences *Akiyo, Foreman, Coastguard, Container, Hall and Mother* are used to fix the threshold in order to balance the tradeoff between perceptibility and robustness. Two experiments are performed to fulfill the aim. First simulation is carried out to estimate the similarities (NC) of extracted watermark at discrete interval of threshold as exposed in Figure 8 and second experiment evaluates the visual quality (PSNR) of watermarked video by varying the threshold as described in Figure 9. It is perceived from the experimental results that more than 30dB of PSNR and 70% or above NC provide the satisfactory results for perceptibility and robustness issue respectively for any video watermarking scheme. From the Figure 8, it is apparent that PSNR is decreasing as increasing the threshold. The average PSNR is 38.6010 obtained at threshold of 0.4 and average NC attained is 0.99985 against the threshold 0.2 considering for all the video sequences. To make the balance between similarity measure and perceptibility, the average threshold is (0.4+0.2)/2 =0.3. NC=1 reflect that 100% watermark is successfully extracted in case of no attack from most of the video sequences as shown in the Table 1.

Table 1. The effect of PSNR and NC on threshold for different video sequences

| Video Clip → | Akiyo | | Foreman | | Coastguard | | Container | | Hall | | Mother | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Thres hold ↓ | PSNR | NC | PSNR | NC | PSNR | NC | PSNR | NC | PSNR | NC | PSNR | NC |
| 0.1 | 47.335 | 1 | 44.314 | 1 | 46.654 | 1 | 45.112 | 0.99978 | 43.8078 | 1 | 48.442 | 1 |
| 0.2 | 44.328 | 1 | 41.113 | 1 | 44.899 | 1 | 41.543 | 0.99989 | 40.7601 | 0.9998 | 44.282 | 1 |
| 0.3 | 43.822 | 1 | 40.674 | 1 | 42.566 | 1 | 39.754 | 0.99984 | 39.3219 | 0.9999 | 42.692 | 1 |
| 0.4 | 41.653 | 1 | 39.001 | 1 | 40.198 | 1 | 37.006 | 0.99967 | 36.2986 | 0.9993 | 40.293 | 1 |
| 0.5 | 36.432 | 1 | 35.433 | 1 | 38.564 | 1 | 33.483 | 0.99956 | 35.7643 | 0.9993 | 38.298 | 1 |
| 0.75 | 34.619 | 1 | 33.112 | 1 | 35.223 | 1 | 31.972 | 0.99944 | 34.5432 | 0.9992 | 35.271 | 1 |
| 1 | 31.956 | 1 | 30.623 | 1 | 30.625 | 1 | 25.675 | 0.9991 | 30.8911 | 0.999 | 32.902 | 1 |
| Average | 40.02 | 1 | 37.753 | 1 | 39.819 | 1 | 36.364 | 0.99961 | 37.341 | 0.9995 | 40.311 | 1 |
| PSNR$_{avg}$ | | | | | | 38.6010 | | | | | | |
| NC$_{avg}$ | | | | | | 0.99985 | | | | | | |
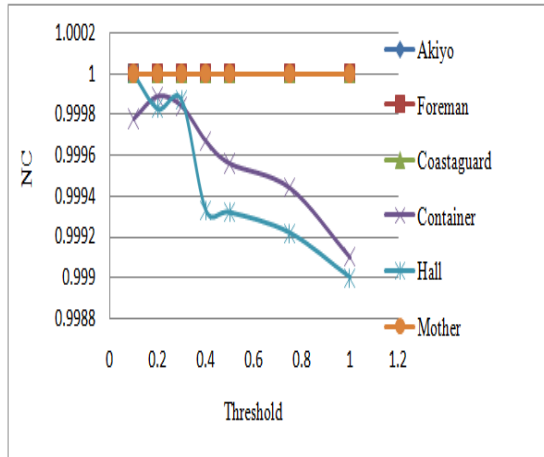
Figure 8.  NC Vs Threshold
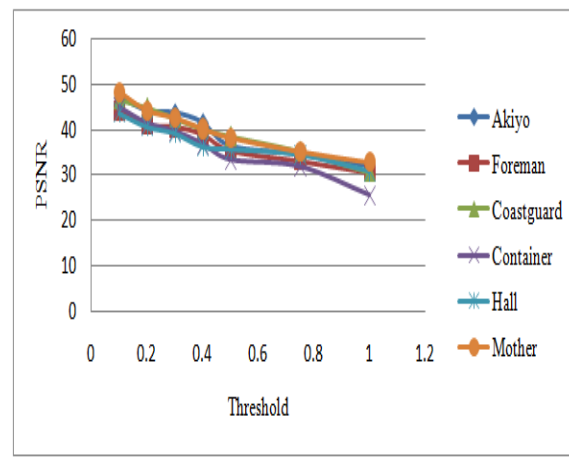


Figure 9.  PSNR Vs Threshold

### 4.2.  Evaluation of Robustness by Applying Intentional and Unintentional Attacks

Several experiments have been evaluated to judge the robustness of the proposed scheme by considering the video Akiyo. To fulfill this purpose, attacks are applied on the watermarked video to retrieve the watermark. The attacks are based on utilizing the properties of video itself. One of the properties of video is its temporal characteristic, the sequence of still images known as video frames. Changing the order of some of the neighboring frames by an attacker insignificant affect on the perceptual quality of watermarked video but corrupt the embedded signal into it.  Another characteristic of video is to contain the large amount of redundancies among the frames. Due to this, frames dropping, frame averaging and frame cropping attacks can be applied to disturb or completely remove the watermark. A cracker can disturb the watermark while preserving the quality of watermarked video by dropping some of the frames and/or replacing the same frames with the original so that the total number of frames will not be reduce. Some of the attacks on video watermarked signal are inherited from image watermarking. These attacks include geometric attacks contains rotation and cropping and various noise insertion attacks as *Speckle noise*, *Gaussian noise*, *Salt and pepper* noise *and Poisson noise*. The proposed scheme simulated the robustness against all above defined attack.
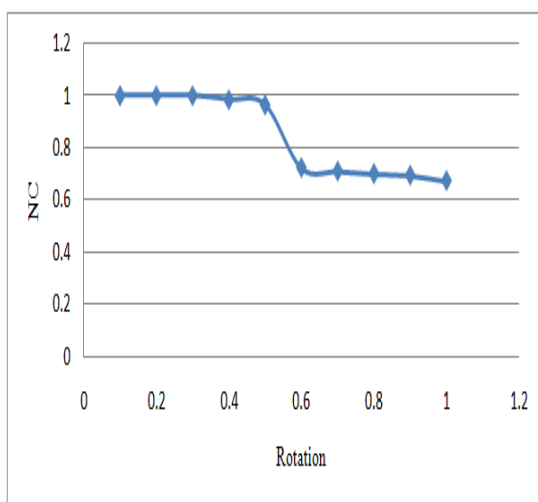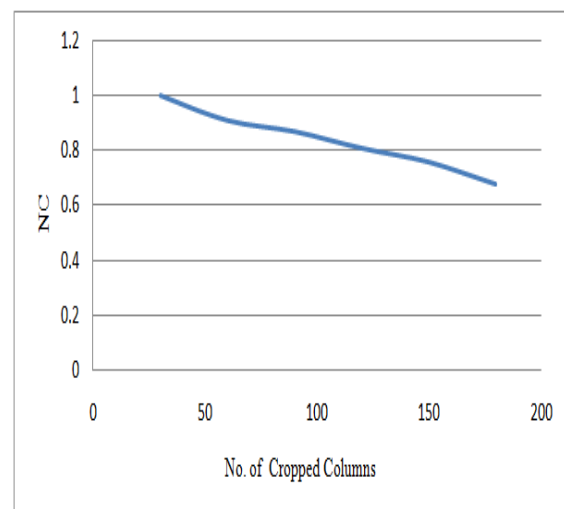


Figure 10. NC Vs Rotation (°)



Figure 11. NC Vs Cropping

### 4.2.1.  Frames averaging attack

Another significant video watermarking attack is frame averaging attack. Average of numerous frames will eliminate the composition of the watermark. It indicates that the current frame is replaced with the average of its own, previous and next adjacent frame. 25% of the watermarked video frames are averaged

to judge the performance of the scheme. It indicates that every 4th watermarked frame is averaged with its two just neighboring frames and resultant frame is replaced with the current one.

### 4.2.2. Frame swapping attack

Frame averaging can also obliterate the watermarked video and therefore affect the extraction quality of watermark. It expressed by defining $F_k = F_k - 1$ and $F_k - 1 = F_k$. Again, 25% of the watermarked video is passes through this attack. In this experiment, every fourth frame is swapped with its next neighboring frame. As the swapping process is started from the first frame, 50% of the watermarked I-frames were replaced with just ahead non watermarked B-frames. The effected I-frames are $1^{st}$, $21^{st}$, $41^{st}$, $61^{st}$, $81^{st}$, $101^{st}$, $121^{st}$, $141^{st}$, $161^{st}$, $181^{st}$, $201^{st}$, $221^{st}$, $241^{st}$, $261^{st}$, $281^{st}$.

### 4.2.3. Frame dropping/ replacement attack

One of the properties of video is the existence of redundancy in its frames. By using this characteristic, a malicious user select some frames from different part of watermarked video and can drop in two different ways. In the first case, the selected video frames were dropped permanently from watermarked video and in other case the selected frames were replaced by their corresponding original frame. In both the cases, an attacker takes care the perceptibility of watermarked video must not be degraded significantly. The experimental simulation is carried out for both the cases. To fulfill this purpose, 25% of the frames are removed from the watermarked video which eliminates the $11^{th}$, $21^{st}$, $31^{st}$, $41^{st}$, $61^{st}$, $71^{st}$ watermarked I-frames also. The second case also replaced the first 25% of the watermarked frames from the frames of original video. It replaced the $11^{th}$, $21^{st}$, $31^{st}$, $41^{st}$, $61^{st}$, $71^{st}$ watermarked I-frames from the corresponding original non-watermarked I-frames.

### 4.2.4. Noise, Filtering and Compression Attacks

Adding noise into the watermarked video is another way to judge the robustness of the embedded watermark. Four different categories of noises Speckle, Poisson, Gaussian and Salt and Pepper were added in order to test the robustness. Due to this, the adverse affects is to face the difficulties while retrieving the watermark information. The proposed scheme applied multiplicative noise as speckle noise to each watermarked frame by using the following method.

$$Frame_{A_i} = frame_{W_i}(1 + n) \tag{7}$$

$frame_{W_i}$ denotes the i-frame from the watermarked-video (w), n is the equally scattered random noise with mean zero and variance 0.04 and $frame_{A_i}$ is the resultant corresponding attacked ith-frame. Poisson noise is generated from the watermarked video object itself instead of adding artificial noise. Gaussian noise with zero mean and 0.01 of variance is applied on the watermarked video. As the size of each watermarked frame is 144 x 176=25344, the number of element affected by adding salt and pepper noise with intensity 0.1 is 25344 *0.1= 2534 pixels. On the contrary, median filter is used to remove the noises from the multimedia objects. It is one of the most common unintentional attacks in digital video. By creating the window size of 3x3, the median filter is applied on the watermarked video to extract the watermark. Certainly, the visual quality of watermarked video is degraded significantly due to huge data are lost. However the watermarked is recovered approximately more than 95% . The proposed scheme achieved the high robustness against all noise insertion based attack as shown in the Figure 13.

Compression is another unintentional attack to video watermarking system. As the video consist the large voluminous data in Gigabytes (GB) or Terabytes (TB), therefore the basic requirement is to compress it before transmitting via internet. The watermarked video with bit rate of 15206 kbps is compressed with MPEG-2 compression standard, reduces the data rate by 40% with a bit rate of 989 kbps. However, it is observed from Figure 13 that the watermark is clearly extracted with high NC value. The aforesaid attacks are exploited on the watermarked video object and the outcomes reflects that the proposed scheme obtained an excellent robustness result against a large variety of intentional and unintentional attacks as illustrated in Figure 12 and Figure 13.

### 4.3. Computational Complexity

It is essential to test the proposed watermarking technique under the real-time constraint. In general, base-band based watermarking scheme have limitations to support the real- time requirement as compared to compressed domain. The proposed video watermarking suggested that the embedding and extraction process are carried out to make sure that the selected block is plain 8x8 2D-DCT block and the computation of only AC coefficient while ignoring the rest coefficients from a particular block. The simulation result has been

taken for evaluating the elapsed time of proposed work. The processing time appreciating the above mentioned strategy is approximately 4.10 and 3.32s during embedding and extraction process respectively. Matlab ver. R2010a installed in computer system with configuration Intel® core™ Duo CPU, 1GB RAM and 32bit Operating system obtained these computing times.
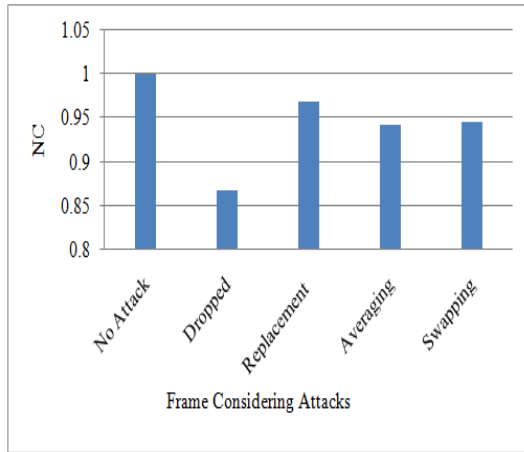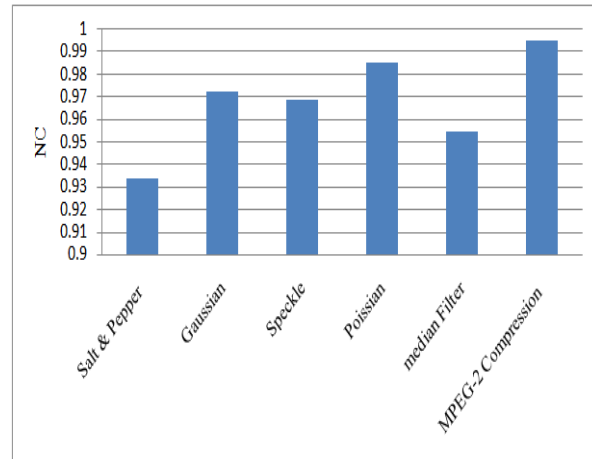


Figure 12. Frame considering Attacks

Figure 13. The effect of robustness against different kind of noises and compression attacks

## 5. STATE OF ART VS PROPOSED METHOD

The concert of the proposed method is compared with existing schemes which are based on compressed domain conveyed in contemporary years. Ming Jiang et al. [9] proposed the video watermarking algorithm to protect the copyright of the video objects. DC coefficient from one 8 x 8 DCT block is responsible for inserting one watermark bit for embedding purpose. The insertion process is depends upon the DC coefficient is odd /even to insert 1/ 0 into it. In this way all the DC coefficients are utilize for embedding purpose. Yong et al. [14] described an adaptive video watermarking process based on human visual system (HVS) and MPEG-4 video compression theory. Low frequency DCT coefficients are utilized to embed the watermark. MPEG-4 video compression is designed for those applications in which low bandwidth are required to transmit the data. D. Badrinath et al. [15 ] suggested the dual video watermarking scheme based on MPEG-2 compression standard. The process of embedding the watermark is based on exploiting the I-frames which is further used to generate the DCT image. The resultant DCT image is added with the DCT of weighted watermark information. The robustness of the proposed scheme is compared with already delivered techniques for the selected attacks as temporal synchronization attacks including frame insertion, frame deletion, frame swapping and frame averaging, signal processing attacks covering various noise attacks as salt and pepper, speckle, Gaussian noise and Poisson noise attacks, median and wiener filtering attacks and recompression attacks. It is observed from Table. 2, the presented scheme offers better robustness compared to other suggested techniques. In addition to the better robustness achieved so far comparing with the existing methods, one major positive aspect of the proposed approach is that the scheme offered good robustness results against unintentional compression attack. The size of watermarked video and compression attacked watermarked video considering 'Akiyo' video sequence is 15.206 MB and 2.35 MB respectively. It reflects that even 85% of the data is lost during re-compression process, still the watermark is recovered almost 100% as shown in the Figure 13. It is because of choosing only the smooth DCT blocks, not all, which is the key idea of the proposed method.

Table 2. The robustness comparison between the presented scheme and previously published algorithms

| S.No. | Type of Attack | Ming Jiang [9] | Yong [14] | Badrinath [15] | Proposed |
|---|---|---|---|---|---|
| 1 | No attack | 1 | 1 | 1 | 1 |
| 2a | 25% Frame dropped | 0.9816 | 0.8520 | -- | 0.8684 |
| 2b | 50% Frame dropped | -- | -- | -- | 0.7927 |
| 3a | 25% Frame dropped and replaced with corresponding original frames | -- | -- | -- | 0.9684 |
| 3b | 50% Frame dropped and replaced with corresponding original frames | -- | -- | -- | 0.9176 |
| 4a | 25% Frame averaged | -- | -- | -- | 0.9425 |
| 4b | 50% Frame averaged | -- | -- | -- | 0.9031 |
| 5a | 25% Frame swapped | -- | 0.8460 | -- | 0.9459 |
| 5b | 50% Frame swapping | -- | -- | -- | 0.8865 |
| 6 | Gaussian Noise ( Mean=0,variance = 10%) | 0.8195 | -- | 0.9104 | 0.9722 |
| 7 | Salt & pepper Noise ( 0.01) | 0.9723 | -- | 0.9012 | 0.9856 |
| 8 | Speckle Noise (0.1) | -- | -- | 0.8218 | 0.9686 |
| 9 | Poisson Noise | -- | -- | -- | 0.9852 |
| 10 | Rotation Attack  (0.5) | -- | -- | 0.96339 | 0.9648 |
| 11 | Cropping Attack (25% column) | -- | -- | -- | 0.9194 |
| 12 | Median Filtering ( 3 x 3) | 0.8770 | 0.8150 | 0.8050 | 0.9546 |
| 13 | MPEG-2 compression | 0.9882 | -- | -- | 0.9953 |

## 6.    CONCLUSION

In this paper, an effective video watermarking method based on classifying the DCT block is proposed. The key design in the proposed scheme is the selection of smooth DCT blocks used for embedding purpose. Furthermore, only single AC pixels out of 63 are exploited from each selected smooth block for insertion and extraction process reflects that most of the DCT blocks and almost entire AC coefficients are not a part of watermarking process but always passes through normal MPEG compression technique which result a good perceptual quality of watermarked video is obtained. The simulation results have shown that the proposed scheme is highly robust against a large variety of signal processing attacks including intentional and unintentional attacks, frame based considering attacks and specially recompression attacks. Due to the semi blind extraction of watermark, the proposed scheme is utilized for public watermarking applications where the original video is not available for extraction process yet three cryptographic keys necessarily required. When security becomes more essential, then all I-frames even P-frames could be chosen for watermarking purpose at a cost of high computational complexity. Besides, the method proposed in the manuscript can be readily extended to other video watermarking applications with only slight revision.

## REFERENCES

[1]    W. Zhu, *et al.*, "Multiresolution Watermarking for Images and Video," *IEEE Transactions on Circuits and Systems for Video Technology*, vol/issue: 9(4), pp. 545-550, 1990.
[2]    Chouhan R., *et al.*, "Fingerprint Authentication by Wavelet-Based Digital Watermarking," *International Journal of Electrical and Computer Engineering*, vol/issue: 2(4), pp. 519-528, 2012.
[3]    H. E. Suryavanshi, *et al.*, "Digital Image Watermarking in Wavelet Domain," *International Journal of Electrical and Computer Engineering*, vol/issue: 3(1), pp. 1-6, 2013.
[4]    A. Houmansadr, *et al.*, "A Novel Video Watermarking Method Using Visual Cryptography," *International Conference on Engineering of Intelligent Systems*, pp. 1-5, 2006.
[5]    Z. Zho, *et al.*, "New algorithm for video watermarking," *International Conference on Signal processing*, vol. 1, pp. 760-763, 2002.
[6]    Y. Ueno, "A Digital Video Watermark Method by Associating with the Motion Estimation," *International Conference on Signal Processing*, vol. 3, pp. 2576-2579, 2004.
[7]    J. McVeigh, *et al.*, "A Software Based Real-Time MPEG-2 Video Encoder," *IEEE Transaction on Circuit and System for Video Technology*, vol/issue: 10(7), pp. 1178-1184, 2000.
[8]    Chung Y. Y., *et al.*, "Development of Video Watermarking for MPEG2 video," *IEEE Procceddings of TENCON*, vol. 10, pp. 1-4, 2006.
[9]    M. Jiang, *et al.*, "Video Watermarking Scheme Based on MPEG-2 for Copyright Protection," *Elsevier Procedia Environmental Sciences*, vol. 10, pp. 843-848, 2011.
[10]  Biswas S., *et al.*, "An adaptive compressed MPEG-2 video watermarking scheme," *IEEE transactions on Instrumentation and Measurement,* vol/issue: 54(5), pp. 1853-1861, 2005.
[11]  V. Saroha, *et al.*, "Enhancing Security of Caesar Cipher by Double Columnar Transposition Method," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol/issue: 2(10), pp. 86-88, 2012.
[12]  J. Jiang, *et al.*, "The Spatial Relationship of DCT Coefficients Between a Block and its Sub-Block," *IEEE Transactions on Signal Processing*, vol/issue: 50(5), pp. 1160-1169, 2002.

[13]  H. Tong, *et al*., "A Perceptual Model for JPEG Applications Based on Block Classification, Texture Masking and Luminance Masking," *International Conference on Image Processing*, pp. 428-432, 1998.

[14]  Yong M., *et al*., "Adaptive Video Watermarking Algorithm Based on MPEG-4 Streams," *10th International Conference on Control, Automation, Robotics and Vision*, pp. 1084-1092, 2008.

[15]  Badarinath D., *et al*., "A Compressed Domain Dual Video Watermarking for Real-Time Applications," *International Conference on Process Automation, Control and Computing*, pp. 1-5, 2011.

## BIOGRAPHIES OF AUTHORS

Rakesh Ahuja is currently working as Associate Professor at Moradabad Institute of Technology, Moradabad, (U.P) India. He is having total twenty one years of experience in the area of industrial, academic, research and administration. He is pursuing the Ph.D degree from IFTM University, Moradabad (U.P) India. He received M.Tech Degree in Computer Science & engineering from Uttar Pradesh Technical University, India and B.Tech degree in Computer Science & engineering trade from BIET Jhansi, (U.P) India. His research interest in development schemes in the areas of cryptography, information and multimedia security for text, video and image by desiging watermarking techniques. He has published several papers in reputed international journals and IEEE conferences.

Sarabjeet Singh Bedi is presently working as senior faculty member in Department of Computer Science and Information Technology, MJP Rohilkhand University Bareilly, India. He is having 18 years of academic, administrative and research work experience. He has received Master of Engineering degree in Computer Science and Engineering with honours from NITTTR, Chandigarh. PhD degree has been awarded to him by Indian Institute of Information Technology, Gwalior, India in Information Technology. His research area includes Network Management and Security, Digital Image Processing. He has published several papers in reputed international/national journals including chapters in edited books. He has received institute medal from Thapar University, India and merit certificate for best paper presentation at World Congress on Engineering, London, U.K, In July 2008.