Indonesian Journal of Electrical Engineering and Computer Science
Vol. 21, No. 2, February 2021, pp. 1160~1167
ISSN: 2502-4752, DOI: 10.11591/ijeecs. v21.i2.pp1160-1167

Compressed domain based robust digital video watermarking scheme to protect the copyright

Rakesh Ahuja, Sachin Ahuja, Deepali Gupta, Mohd Junedul Haque
Chitkara University Institute of Engineering & Technology, Chitkara University, Punjab, India

Article Info

Article history:

Received Jul 3, 2020
Revised Sep 18, 2020
Accepted Oct 2, 2020

Keywords:

DCT
MPEG-2 structure
Signal processing
Video processing
Video watermarking

ABSTRACT

Digital video watermarking is an effective way to protect the ownership of the multimedia contents. A novel compressed domain based digital video watermarking algorithm scheme is proposed by exploiting MPEG-2 structure. Watermark bits are embedded in DC and AC coefficients both of only smooth discrete cosine transform (DCT) blocks from selected I-frames in the original digital video. The algorithms never exploited entire frames but explore only three location from the subset of DCT blocks from the subgroup of I-frames only. This process maintains the perceptibility of the watermarked video. Two parameters, normalized correlation (NC) and bit error rate (BER) are used to evaluate the degree of similarity and dissimilarity respectively to check the robustness against image processing and video specific intentional and non-intentional attacks. The security of embedded watermark is enhanced by applying three cryptographic keys. The experimental results demonstrated that the better robustness and perceptibility achieved by comparing the results with the state of art.

Corresponding Author:

Mohd Junedul Haque
Chitkara University Institute of Engineering & Technology
Chitkara University, Punjab, India
Email: junedul.haque@chitkara.edu.in

1. INTRODUCTION

The rapid growth of digital technology and high internet bandwidth make easier to change, copy and transfer multimedia content from one workstation to other regardless of the terrestrial position. Due to such easiness, another matter arises like piracy, editing, softening and tempering with the original digital multimedia data and also making multiple copies and redistribution in an illegal way and much more thoughtful concern to claim for false ownership or copyright protection. In earlier point of time, encryption technique protects the contents during the transmission. Yet, the technique fails, once the digital contents are decrypted at destination end. The image or video type of object can also be protected by embedding the digital watermark into the original object to keep the imperceptibility and robustness in an efficient manner. It certainly feels more considerable for multimedia owners as well as for clients for sharing such digital contents. There are numerous methods to embed the digital watermark into video and these are depending upon the type of host signal like original signal, compressed or during the compression.

The original video can be considered of two types; First category of video is not compressed at all and other one is to uncompressed the signal before embedding. But, actually, both are identical in nature and measured as the series of separate frames. Therefore, methods used for image watermarking [1-4] can also stretched to video watermarking scheme [5-8] also. Yet, the downside to use the original host signal for embedding is that the bit rate of watermarked contents is increased. On the other hand, watermarking process can be applied to compressed video signal. The advantage of this scheme is that the optimal perceptibility is

obtained at the cost of limited payload capacity of watermark information is allowed otherwise perceptibility issues arises. The third and most suitable way is to apply the watermarking process during encoding [9] the video. It is more realistic approach as it serve dual purpose, compression in parallel to watermarking process. The video is consisting of enormous redundant data and hence required to be compressed essentially in order to minimize the storage capacity as well as to optimize the internet bandwidth before sending to another system or to store into the local host. The benefit associated with this process is that neither compression nor decompression is required before or after compression of the video for embedding purpose. Hence, the purpose of the proposed technique is exploiting the compression process to insert the watermark while encoding the video type of multimedia object to fulfil all three basics challengingnecessities of toughness, throghput and imperceptibility.

The organization of paper is planned into seven sections. The brief introduction for digital watermarking for video elaborated in Section 1. Section 2 explained about the compression scheme of MPEG-2 video. Section 3 is set for literature review related to video watermarking scheme. A robust digital watermarking schemefor video object proposed in Section 4. Section 5 eloborated the experimental setup and associated results and discussion. Section 6relate the outcome of the proposed technique with the state of art. The limitations and future works discussed in Section 7.

2. BACKGROUND OF MPEG-2 VIDEO COMPRESSION STANDARD

The advancement ofcoding procedureof MPEG-2 [10] started in 1990. The sequence of video frame is partitioned nto group known as group of pictures (GOP). Each GOP contains threedissimilar categories of frames namely I-frames (Intra) also known as Intra-coded types of frames, P-frames as forward predicted frames and B-frames (Bi) defined as bidirectional frames. The order of usage of all kind of frames within the same GOP are shown in the Figure 1(a) and Figure 1(b) during compression and decompression respectively.

FrameNo	1	2	3	4	5	6	7	8	9	10
Frame Type	Intra	Bi	Bi	P	Bi	Bi	P	Bi	Bi	P

(a)

FrameNo	1	4	2	3	7	5	6	10	8	9
Type	Intra	P	Bi	Bi	P	Bi	Bi	P	Bi	Bi

(b)

Figure 1. (a) Display order of GOP, (b) Processing order of GOP

Each video frame is further partitioned into unit of a macroblocks for processing. The activation of mode of macroblock is depend on the category of frame to process. If I-frame, each macro block having size of 16x16 is segregated into number of blocks of same size of 8x8. Every block of each I-frame takes participates in encoding process and therefore they always serve as necessary key steps to encode the video data. I-frames do not take the reference from forward or previous frames and hence encoded directly. The type of P-frames is encoded by taking the reference from previous P-frame or I-frame. It provides more compression then I-frames. The consequence is P-frames are more complex than I-frames. B-frames exploits future and past framereferences both. The reference frames may be the combination of I-frame and P-frame P-frames and B-frames orboth P-frames provides maximum compression.

The encoding structure of MPEG-2 alienated into three mainshares: Extraction of DCT coefficients, evaluating motion vectors and header information. There are number of ways to exploits these major parts forwatermarking purpose also but first two are more prominent way to do so. First approach suggested that if I-frames to be processed then video frame is passes through DCT followed by quantization operation. Subset of the coefficients of DCT blocks are utilized to insert binary watermark bits, especially when blind watermarking needed. In general, I-frames consisting large number of DCT coefficients therefore high payload capacity of watermark bits can be exhausted. Since I-frames reflects most of the information therefore considered as potential frames as compared to P-frames or B-frames.

The proposed scheme exploited I-frames while compressing the video through MPEG-2 standard to insert the copyright data. It designed carefully so that the superiority of watermarked video must not be tarnished sharply as well as the scheme also balance the tradeoff among perceptibility, payload and robustness.

3. RELATED WORK

Ting Hsu et al. [11] altered the quantized intermediate DCT frequency coefficients to embed the watermarking bits by practicing the MPEG structure. The limitation associated with the approach is that is

the adjustment of DCT coefficients is highly depends upon the quantization process. The watermark is inserted by using the spread spectrum technique by Bijan G. Mobasseri [12]. They extracted the watermark by decodeding the bit stream from the MPEG-2 compression standard. The limitation of the approach is that the very less payload capacity would be allowed. You-Ru Lin et al. [13] explained thealgorithm based on block matching as per the direction of motion vectors. The advantage of the scheme is that the extarction of watermark is possible blindly. Satyen Biswas et al. [14] defined video watermarking algorithm based on the structure of MPEG-2. Each scene of the movie is used to embed each partitioned image. The different parts of watermark are inserted intodifferent frame of video. The limitation is that only I-frames are exploited for this purpose, but when security is concerned all three types of frames I, B and P could beused at the cost of computational time. Lu Jianfeng et al. [15] elaborated the video watermarking scheme grounded on DCT coefficients. They adapted the coefficients of DCK block to insert the watermark bits. Little enhancing the controlfeature, extremely degrade the quaity of watermarked video. Ahuja et al. [16] stretched the work by exploiting the MPEG2 structure to cover the above limitations. They also focused on efficiency of the watermark scheme by calculating the elapsed time. Yoshito Ueno et al. [17] inserted the watermark image by first extracting the macro block of Cr or Cb and Y components of I-frame when motion vectors belong to P-frames and then embedding the watermarking bits by little modifying these vectors. The limitation is that the tradeoff among the three essential parameters is not obtained in a heightened manner. Yuk Ying Chung et al. [18] quantized the DCTvalues by exploring the MPEG-2 structure. The least significant bit of the DC coefficient is used to insert the watermark bit. The drawback of this scheme is that the assailant may completely collapse the watermark by randomizing the LSB of DCT blocks. Daniel Cross et al. [19] anticipated the watermarking method to evaluate authentication of MPEG video. The algorithm identified the carrying VLCs to embed the watermark object. Anil kumar Sharma [20] explored the quantization index modulation technique for inserting the watermark bits into P-frames. Since construction of P-frames have a very less space to insert anything additionally. Therefore, robustness issue always be a challenge while desigining watermarking method using MPEG structure.

To overcome these limitations, the proposed method embeds the watermark bits by exploiting both DC and AC coefficients of only smooth types of 8x8 DCT blocks from randomly selected I-frames. The novelty of the proposed scheme is that neither entire I-frames nor entire DCT blocks are chosen. Moreover, different techniques are employed to insert the encrypted watermarking bits in DC and AC coefficients both. Therefore, the proposed approach not only enhanced the security of watermark object embedded into the video but also the balanced tradeoff is obtained among all three parameters.

4. PROPOSED VIDEO WATERMARKING ALGORITHM

Proposed digital video watermarking scheme is broadly classified in four major categories as Watermark encryption and cryptographic key generation algorithm, creating a vector of I-frames, embedding algorithm and extraction algorithm.

4.1. Watermark encryption and key generation

The scheme suggested to have four keys used in watermark extraction process to provide more secure algorithm. First key is used to stop the watermark extraction algorithm and other two keys are used to exhibit the extracted watermark object from the watermarked video. Fourth key is used to encrypt the watermark and issynchronized between sender and receiver. Since three keys are generated from the watermark itself and additional single key is used for encryption of watermark itself. Therefore, high level of security is provided to secure the watermark from malicious user. First key is extracted from the size of encrypted watermark object measured as*Pixels*. Second and third keys are generated from the dimensions of the encrypted watermark are as*Rows and Cols*. Fourth key, say *Symmetric*, is depend upon the the permutations of the column and shall be used to encrypt the watermark by using usingdouble column transposition method [21].

4.2. Creation of vector array of i-frames

The original video is segregated into the group of pictures (GOP) consisting I, P and B-frames. The general structure of MPEG-2 suggested to have 10 frames in single GOP and I-frame must be followed by a chain of P-frames and B-frames but it doesn't necessary to follow the same sequence. It depends upon the frame that have drastically change from previous frame whether it may be P-frame or B-frame. There may be the state when P-frame may have extremely deviate from the previous I-frame or P- frame and therefore it may be predicated awful and due to which it is better to encode it as I-frame.

4.3. Watermark embedding process

Since I-frames are having less compression ratio and high density of DCT blocks as compare to P and B frames therefore the proposed scheme uses the same type of frames to insert the watermark bits by little modifying the DC and AC value of each plain DCT blocks of Y component of individual I-frame in view of that the superiority of video not be spoiledexpressively. The embedding algorithm is defined as follows:

1) Read encrypted watermark image and store its entire bits into vector array as *W-Bits.* Update *W-Bits* by adding the sufficient bitsso that total number of bits can be divisible by three.
2) Initialize the vector array *I-framesArray*and obatined the total number of I-frames and store in *N*.
3) Pick three adjacent watermark bits from *W-Bits* to be adjusted into one DC and two AC coefficients into the currently selected plain DCT block.
4) Apply the Fibonacci seriesalgorithm to generate the frame number as *FNo* in such a way that the value must be unique, not repeated and less than or equal to N
5) Put the sequence number of *FNo*in the array *Seq Ran SelectedI-Frames*.
   a) *FNO* is categorized into luminance (*Y*), Chroma blue (*Cb)*andChroma Red *(Cr*) components.
   b) Choose *Y* channel as this is the most luminance part contains maximum energy
   c) Split the Y matrix into the blocks of same size (8x8) for applying DCT followed by quantization.
   d) Check the quantized DCT for plain type. If not, then select next adjacent DCT block.
   e) To insert three watermark bits at a time, follow the following steps. First watermark bit from a set of three bits, will be inserted into DC coefficient by adjusting its value. Check the DC coefficient for even or odd. If it isodd integer and the picked watermark bit is *1 or*if it is even and the picked watermark bit is 0 then no change in DC value. Pick rest two watermark bit jointly. The combination may be 00, 01, 10 or 11. Pick up two AC values from the location (7,8) and (8,8). If both these values are also zero then no change at all and it considered as both watermark bit have been inserted otherwise make them zero else if the watermark bits are the combination of 01 then check if (7,8) is lower than (8,8) then no change in the current AC values and considered as two values are entered otherwise make (7,8) must be less than (8,8) else if the watermark bits are the combination of 10 then check if (7,8) is greater than (8,8) then no change in the current AC values and considered as the pair of 10 is inserted otherwise make (7,8) greater than (8,8) else the remaining option is the pair of bits are 11 can be considered as inserted if both AC value are nonzero and equal.
6) If entire watermark bits have not exhausted then Go to step v-d to pick next DCT block to insert next three adjacent bit
7) AdjusteSeq*RanSelected I-frame* to their original sequential order and replaced watermarked I-frames with original one. Continue with MPEG algorithm and get Watermarked Video as WtrVdo.

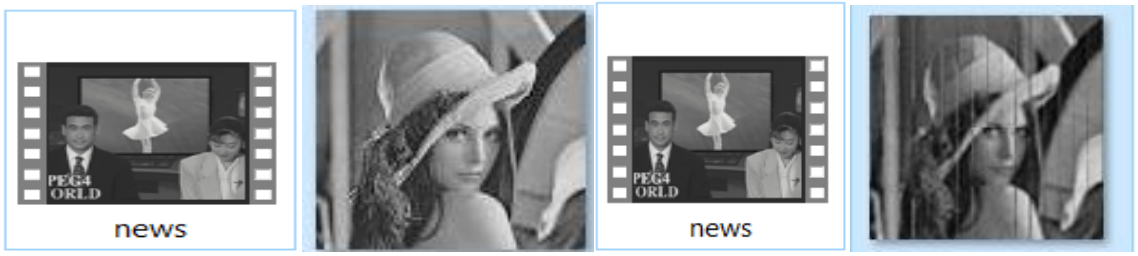
4.4. Watermark extraction process

1) Read Watermarked Video *WtrVdo* to get the sequence of entire watermarked I-frames.
2) Apply the Fibonacci seriesalgorithm to select the actual watermarked frame number as *FNo* in such a way that the value must be unique, not repeated and less than or equal to N until the loop completed the round equal to N.
3) The chosen I-frame *FNO* is categorized into three components are Y, Cb and Cr components.
   a) Choose *Y* channel and split into equal size of blocks and apply DCT.
   b) For each DCT block, check for smooth type of DCT block. If not pick another DCT block.
   c) The odd value of DC extracted the watermark bit *1* else *0*. Two more locations (7,8) and (8,8) are processed to getone pair of bits. If both ACvalues are also zero then increment the vector array of extracted watermark as 00 into 2 more adjacent location of an array. if (7,8) is lower than (8,8) then augmented the array with 01 else if (7,8) is greater than (8,8) then filled the array of next two location with 10 else if both AC value are nonzero then increment the array of extracted bits with 11.This method extracted three bits from the same DCT block.
   d) Choose another DCT block to extract three more bits. If size of extracted watermark is equal to the size of key *SIZE* then stop the extraction process otherwise select next adjacent DCT block.
4) Convert vector array into 2- dimensions array by using two another key *Rows* and *Cols*to display the extracted watermark image from watermarked video

5. EXPERIMENTAL SETUP AND RESULTS ANALYSIS

The static video *News* is used to evaluate the simulation results. The snapshot of the video clip is illustrated in Figure 2(a). The frame rate and the length of the *News*are 25 frames/second and 300 framesrespectively. 176x144 is the size of each video frame. A binary watermark *Lina as* watermark is

shown in Figure 2(b) is chosen for embedding purpose. The size of this image is 122 x 127 with bit depth 1. This image is embedded into the video clip of *News* in such a manner that the quality of watermarked video will not be affected drastically. The snapshot of the watermark video is illustrated in the Figure 3(a). The extracted watermark from the watermarked video is shown in Figure 3(b). The simulation results have been evaluated for three major parameters as defined below.



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

Figure 2. (a) Frame no. 10 of figure, (b) original watermark figure, (c) frame no. 10 of figure, (d) extracted watermark original video watermarked video

5.1. Perceptibility

The perceptibility factor measures the degree of similarity between the original video with the watermarked video. It is defined by the following formula.

$$PSNR = 1/Frames \sum_{K=1}^{NoofFrames} PSNR_L \quad (1)$$

Where $PSNR_L$ = 10 $\log_{10}$ 255/ MSE_K termed as Peak Signal to Noise Ratio. PSNR is measures between L^{th} originalframe and L^{th} Watermarked Video frame and MSE it is defined as mean square error between these two frames, defined by the following formula –

$$MSE_K = 1/MN \sum_{i=0}^{N-1} \sum_{J=0}^{M-1} ((OriginalVid(i,j)_K - WaterVid(i,j)_K)^2 \quad (2)$$

M x N is the magnitude of video frame and OriginalVid(i,j) focused to specific pixel value of i^{th} row and j^{th} column of original video frame ($OriginalVid(i,j)_K$) and WaterVid(i,j) mentions to specific pixel value of i^{th} row and j^{th} column of watermarked video frame. The proposed algorithm calculated the PSNR between original and watermarked video with and without attacks as shown in the Table 1.

5.2. Robustness

1) Normalized coorelation: The robustness parameters calculate the degree of similarity between extracted and original watermark. It is defined by the normalized correlation as defined below:

$$NC = \frac{\sum_{i=0}^{A-1} \sum_{j=0}^{B-1} Wt(i,j) Wt'(i,j)}{\sum_{i=0}^{A-1} \sum_{j=0}^{B-1} Wt(i,j)^2} \quad (3)$$

2) Bit Error Rate (BER): It measured the dissimilarities between the extracted and actual watermark image. In general, it is not known the threshold value for which the value is acceptable

$$BER = \frac{\sum_{0}^{M-1} \sum_{0}^{N-1} Wt(i,j) \oplus Wt'(i,j)}{MN} * 100 \quad (4)$$

The original watermark is Wt and extracted watermark is Wt'. A x B is the size of watermark image. The robustness is evaluated by evaluating NC and BER both. The association between them is that BER is not directly propositional to NC. As NC increases BER reduces shows that the robustness results are good with respect to robustness. Simply, when NC equivalent to zero and BER found to be one reveals that either watermark not present or it cannot be extracted. On the contrary, if NC exhibit to one and BER to zero then there is no noticeable alteration amid the original and the extracted watermark.

The digital video watermarking method passes through the wide variety of following spatial and temporal video and image processing types of attacks image processing and video editing attacks are applied attacks such as image processing attack and video specific attacks. Robustness of the proposed algorithms has been tested through simulation of the following attacks:

3) Spatial synchronous attacks
   a) Geometric Attacks: Cropping, Rotation, Resize
   b) Noise Attacks: Gaussian Noise, Speckle Noise, Salt & Pepper Noise
   c) Filtering Attacks: Median Filtering Attacks, Wiener Filtering Attacks
4) Temporal synchronous attacks
   a) Video Manipulation Attacks: Frames insertion, deletion, averaging, swapping and replacement.
   b) Data Compression Attack: Cinepak Attack

Finest robustness outcomes are obtained against frame deletion, averaging, replacement, swapping and frame insertion attacks as compared to other listed attacks. Frame replacement is one of the important attacks and it is applicable for those circumstances where the commercial advertisement is inserted by replacing the less important original video frames from the watermarked video with the condition is that the entire length of the video must not be enhanced. The sturdiness of the projectedtechnique tested to extract the watermark by applying various types of noises inserted into the watermarked video. The results are good for the small value of noise addition into the watermarked video. As far as geometric attack is concern two attacks namely *rotation attack* and *crop attack* are very most important attacks. Best results of extracted watermark in this algorithm are shown in Table 1. The watermark is fruitfully extracted after rotating the entire video frames by 0.1°. The result shows that the perceptibility is decreasing while increasing the angle of rotation attack beyond 0.1°. Absolutely, the robustness is increases by the rotation detector at the cost of complexity increases. The cropping attack provides satisfactory results for cropping frames less than or equal to 10%. The proposed scheme measured the BER, NC and PSNR with and without attacks as per the Table 1 listed.

Table 1. NC, PSNR and BER

	(NC)	(PSNR)	(BER)
No Attack	0.98343	41.3398	2.5400
Rotation	0.89419	40.6641	12.1419
20% frames cropped	0.91403	39.9923	8.8849
Speckle Noise	0.91034	39.6865	8.7337
Salt & Pepper Noise	0.96446	39.3036	3.3532
Gausian Noise	0.8385	37.4524	16.2974
Median Filter	0.8335	37.7444	28.3974
Frame Replacement	0.94187	38.0504	6.6534
Frame Insertion	0.79888	36.3380	22.4382
Frame Deletion	0.96228	38.2234	4.3518
Frame Swapping	0.94197	38.1402	5.8143
Frame Averaging	0.95343	38.0026	4.5427
Compression	0.7127	37.4866	23.0109
Wiener Filter	0.69956	36.4757	28.3974
Median Filter	0.96233	38.455	0.4322

6. STATE OF ART VS. PROPOSED SCHEME

The outcome of the schemecontrastsby the techniques adopted by researchers either compressed or uncompressed domain-based technique both as shown in Table 2. Some of the researchers judge the robustness by measuring NC and other evaluated BER. In order to do perfect comparisons, the proposed technique appraised the mentioned parameters of NC as well as BER so that the experimental results can be truly compared for those evaluated only NC or only BER or both. On the other hand, the quality of watermarked video also checked after applying wide varieties of image and video processing attacks. The third parameter is to evaluate the payload capacity in the proposed technique. Three watermark bits from a single quantized DCT block will be inserted.

The following observation were made.

a) The better resultswere obtained than the schemes suggested by previous researchers for image level attacks as geometric attack, various noise attacks andvideo specific attacks.
b) The perceptibility of watermarked video is contrast with the original video tested demonstrated in the Table1. The range of value obtained between 36.4757 (with attack) and 41.3398 (without attack), shows that perceptibility has not degraded sharply even in worst case.

c) The robustness results are almost better than previous work as described. The results are tarnished only for speckle noise attack only shown by bold case letter with respect to [17].
d) The nature of key varies for each watermark. It reflects that the watermark can never be edited or remove by the invader until cryptographic keys are compromised along with the nature of algorithm.

Table 2. Proposed vs state of art result

S. No	Attack Type	[22]		[23]		[24]		[25]		Proposed Scheme		
		PSNR	NC	PSNR	NC	PSNR	BER	PSNR	NC	PSNR	NC	BER
1	Rotation	---	0.85	---	0.76	---	45.87	---	0.914	40	0.89	15.8419
2	Cropping	---	0.86	---	0.73	---	6.52	---	---	39.99	0.91	8.849
3	Speckle Noise	---	0.94	---	0.91	35.04	11.34	---	---	39.68	0.91	3.3530
4	Salt & Pepper	---	0.93	---	---	34.67	---	---	0.668	38.30	0.93	6.3429
5	Gaussian	---	0.81	---	---	---	---	---	0.684	37.45	0.83	16.290
6	Median Filter	---	0.54	---	0.63	35.04	6.54	---	---	37.74	0.83	28.391
7	Wiener Filter	---	---	---	---	35.04	---	---	---	36.47	0.69	28.391
8	Frame Replacement	---	---	---	---	---	---	---	---	38.05	0.94	6.653
9	Frame Insertion	---	0.69	---	---	---	---	---	---	36.33	0.79	22.43
9	Frame Insertion	---	0.69	---	---	---	---	---	---	36..33	0.798	22.43
10	Frame Deletion	---	0.90	---	---	---	---	---	0.880	38.22	0.96	4.3518
11	Frame Swapping	---	---	---	---	---	---	---	0.901	38.14	0.94	5.8143
12	Frame Averaging	---	---	---	---	---	---	---	0.9030	38.00	0.953	4.5427
13	Compression	---	---	---	---	---	28.13	---	---	37.47	0.712	23.0109

7. CONCLUSION

This paper elaborates the DCT based technique of digital video watermarking in a robust and imperceptible mannerusing the MPEG structure. Robustness results are successfully evaluated against various noise attacks, compression attack, and frame-based attack whetherdeliberatlyor non-deliberately attacks. The beauty of this proposed algorithm is that the watermark can withstand even after applying any one of the attack or more mentioned above andextracted effectively with no significant effect on perceptibility. The future work suggested to examine more test to judge the robustness against collusion attacks type-1 and type-2, composite and ambiguity attacks.

REFERENCES

[1] S. S. Bedi and S, Verma, "A design of secure watermarking scheme for images in spatial domain," *Proceedings Annual IEEE India Conference*, pp. 1-6, 2006.
[2] S. S. Bedi, R. Bano, and S, Verma, "Secure digital image watermarking scheme for copyright protection and buyer fingerprinting," *Proceedings of the World Congress on Engineering, WCE,* London, vol. 1, 2008.
[3] A. Haj, Ali, and A. Mohammad, "Crypto-watermarking of transmitted medical images," *Journal of digital imaging*, vol. 30, no. 1, pp. 26-38, 2017.
[4] A. Haj, Ali, and H. A. Nabi, "Digital image security based on data hiding and cryptography," *In 2017 3rd International conference on information management (ICIM), IEEE*, pp. 437-440, 2017.
[5] S. Almuzairai and N. Innab, "Video watermarking system for copyright protection based on moving parts and silence deletion," *International Journal of Advanced Computer Science and Applications*, vol 10, no. 2, pp. 640-655, 2019.
[6] M. Jiang, Z. Maa, X. Niua, Y. Yanga, and Y. Xian, "Video watermarking scheme based on mpeg-2 for copyright protection," *Procedia Environmental Sciences*, vol. 10, pp. 843-848, 2011.
[7] M. Asikuzzaman and M. R. Pickering, "An overview of digital video watermarking," in *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 28, no. 9, pp. 2131-2153, Sept. 2018, doi: 10.1109/TCSVT.2017.2712162.
[8] Dhaou, Dorra, S. B. Jabra, and E. Zagrouba, "A multi-sprite-based anaglyph 3d video watermarking approach robust against collusion,"*3D Research*, vol. 10, no. 2, p. 21, 2019.
[9] Ahuja, Rakesh, M. J. Haque, S. Tanwar, N. Gautam, and A. Rana. "Secure and robust watermarking scheme based on motion features for video object," *2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO). IEEE*, pp. 146-151, 2020.
[10] V. D. Meer., "MPEG-1 Systems: Laying the MPEG-2 foundation," *Fundamentals and Evolution of MPEG-2 Systems: Paving the MPEG Road, Wiley*, 2014.
[11] C. T. Hsu and J. L. Wu, "DCT-based watermarking for video," *Consumer Electronics, IEEE Transactions on*, vol. 44, no. 1, pp. 206-216, 1998
[12] B. G. Mobasseri., "A spatial digital video watermark that survives MPEG," *In Proceedings International Conference on Information Technology: Coding and Computing, IEEE*, pp. 68-73, 2000.
[13] Y. R. Lin, H. Y. Huang; W. H. Hsu, "An embedded watermark technique in video for copyright protection," *ICPR. 18th International Conference on Pattern Recognition*, vol. 4, pp. 795-798, 2006.

[14] S. Biswas, S. R. Das, and E. M. Petriu, "An adaptive compressed MPEG-2 video watermarking scheme," *IEEE Transaction on instrumentation and measurement*, vol. 54, no.5, pp. 1853-1861, 2005.
[15] L. Jianfeng, Y. Zhenhua, Y. Fan, L. Li, "A MPEG2 video watermarking algorithm based on DCT domain," *Workshop on Digital Media and Digital Content Management*, pp.194-197, 2011.
[16] R. Ahuja, S. Sbedi, "Copyright protection using blind video watermarking algorithm based on MPEG-2 structure,". *In IEEE proceedings of conference*, pp. 1048-1053, 2015.
[17] Y. Ueno., "A digital video watermarking method by associating with the motion estimation," *IEEE Proceedings. ICSP, 7th International Conference on Signal Processing*, vol. 3, pp. 2576-2579, 2004
[18] Y. Y. Chung, F. F. Xu, F. Choy, "Development of digital video watermarking for MPEG-2 video," *Proc of IEEE*, pp. 1-4, 2006.
[19] D. Cross and B. G. Mobasseri, "Watermarking for self-authentication of compressed video," *IEEE proceeding, International Conference*, vol. 2, pp. 913-916, 2002.
[20] A. K. Sharma and Y. M. Pervej, " Simulation and analysis of digital video watermarking using MPEG-*2*," I*nternational Journal on Computer Science and Enginee*ring, vol. 3, no. 7, pp. 2700-2706, 2011.
[21] S. Vinod, S. Mor, and A. Dagarb, "Enhancing security of Caesar cipher by double columnar transposition method," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 2, no. 10, pp. 86-88, 2012.
[22] R. Ahuja and S S. Bedi., "Video watermarking scheme based on candidates i-frames for copyright protection," Indonesian *Journal of Electrical Engineering and Computer Science*, vol. 5, no. 2, pp. 391-400, 2017.
[23] H. H. Mirza, H. D. Thai, Y. Nagata, Z. Nakao, "Digital video watermarking based on principal component analysis," *Innovative Computing, Information and Control, 2007. IEEE Second International Conference on ICICIC*, pp. 290-290, 2007.
[24] Y. G. Wang, Z M. Lu, L. Fan, Y. Z. Robust, "Dual watermarking algorithm for AVS video," *ELSEVIER, Signal processing image communication*, vol. 24, no. 4, pp. 333-344, 2009.
[25] L. Rajab, T. A. Khatib, A. A. Haj, "Hybrid DWT-SVD video watermarking," *IEEE proceedings, international conference*, pp. 588-592, 2008.

BIOGRAPHIES OF AUTHORS

Dr Rakesh Ahuja havingPhD degree in the the field of Computer Science & Engineering. He is having experience of 24 years in Administration, Acedemic, Research and and Industries. His research area includes Digital Right Management, Multimedia Security, Pattern recognition and Information Hiding. His teaching interest is in Distributed System, Real Time System, Software Engineering, Operating System, Database Management System and Computer Programming in C, Object Oriented Programming in Java. He has published more than 30 research papers in National &International journals and Conferences.

Dr. Sachin Ahuja, PhD in Computer Science and Engineering. His specialization is in Data mining. Particularly, he is expertise in survey questionnaires, predictions andevaluating the academic concert of students and judgement of professional teaching with tossed and mixededucation models. In addition to data mining, his teaching interests include relational database, procedural languages and Big Data. Moreover, he is a convener of Patent Facilitation andalso facilitate the inventors in filing patents by administrative them in consultancy and licensing.

Prof. (Dr.) Deepali Guptais Ph.D in Computer Science & Engineering. She is Professor Research in Chitkara University Research and Innovation Network (CURIN) at Chitkara University, Punjab, India. Herarea of interest is cloud computing, machine learning and software engineering. She has published more than 60 research papers in journals and conferences. Dr. Deepali has worked on various administrative positions like Chairman SC/ST Cell of MMU, Sadopur and Principal(MMGI, Sadopur)

Dr. Mohd Junedul Haque is working as an Assistant Professor in the Department of ChitkaraUniversity Research & Innovation Network at Chitkara University, Punjab India. His areas of expertise are Image Processing, Multimedia Technology, CloudComputing, Internet of Things, Data Mining and Data Warehousing. He has published around 20 research papers inInternational Journals and conferences and also, he is an author for 4 books