2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)
Amity University, Noida, India. June 4-5, 2020

Secure and Robust Watermarking Scheme based on Motion Features for Video Object

Rakesh Ahuja
Chitkara University Institute of Engineering and Technology
Chitkara University Punjab, India
rakesh.ahuja@chitkara.edu.in

Purnima
Chitkara University Institute of Engineering and Technology
Chitkara University Punjab, India
purnima.arvind@gmail.com

Mohd Junedul Haque*
Chitkara University Institute of Engineering and Technology
Chitkara University Punjab, India
*junedul.haque@chitkara.edu.in
*Corresponding Author

Sarvesh Tanwar
Amity Institution of Information Technology
Amity university,
Noida, Uttar Pradesh
s.tanwar1521@gmail.com

Nidhi Gautam
University Institute of Applied Management Sciences
Panjab University, Chandigarh
nidhig121@gmail.com

Ajay Rana
AIIT, Amity University Uttar Pradesh
Noida, India
ajay_rana@amity.edu

***Abstract*— The rapid development of worthy internet bandwidth transfers the digital multimedia objects to remote computer system instantaneously. The advent of digital technologies makes possible to create multiple identical copies of the original video. These two revolutionary changes in technologies exploited by malicious user also to make false claim for ownership protection, copyright protection, copy control and many more issues. The proposed technique suggested an innovative method by embedding the different segments of scrambled watermark in the extracted motion features of the video. The encryption key used to encrypt the watermark is depend upon the features of video and it always different for each different video. The scheme is robust and imperceptible enough to secure the watermark embedded into the video object. The outcome reveals that the scheme is robust to intentional and unintentional image and video specific attacks considered to occur frequently in nature. The superiority of the algorithm is that it found better robustness against compression attack.**

Keywords*— Copyright Protection, Discrete Cosine Transform, Digital Video Watermarking, Motion Frames, Multimedia Security, Singular Value Decomposition.

I. INTRODUCTION

The advent of high bandwidth of internet makes easier to share the multimedia objects by means of audio, video, image and text to remote workstation instantaneously, regardless of their terrestrial location with no compromise of security and quality. The advancement of multimedia technology, digital technologies and quick internet services introduces several issues as creation of several identical copies, tempering, false ownership and redistribution of same or tempered contents to unauthorized customer. Therefore, perfect solutions are required to protect the ownership, copyright, authenticity, security and replication of the source multimedia type of documents. The cryptography algorithms protect the contents in transit mode so that the malicious user neither access nor adjusted the unintelligent form of source content. The concern associated with this approach is that once the data is decrypted at receiver end then it becomes the original one. Therefore, the technique fails to protect the data from receiver itself to reproduce and replicate the multimedia content. Therefore, a crucial prerequisite needed to develop a technique to avoid misuse of received information like creation of illegal reproduction, tempering, retransmitting and false claim for ownership or copyright. The advent of digital watermark technology is providing feasible solution for last two decades. Yet, some of the challenges still exist.

Digital watermarking is a technique to hide the external information into the host signal with the aim that a relationship must exist between the host signal and external information. The copyright information as watermark can be embedded into the video object in order to proof the copyright after extraction of the same as and when any unauthorized. Other major requirements are to maintain the balance tradeoff among the perceptibility, robustness and payload capacity. The embedded signal must be robust enough so that it cannot be destroyed by any unlawful person nevertheless can be extracted by the authorized person to proof for copyright protection or ownership. The additional information required to embed into the cover object depends upon the type of application and accordingly watermark information embedded into the cover data. The categories of embedded signal may be owner name, signature, logo, copyright, serial number, copy control signal, binary images, gray level images, color images, text, distributor name, customer name, transactions dates or other applicable digital formats. These watermark signals are used in a wide variety of watermarking applications [1] includes broadcast monitoring, fingerprinting, copyright protection, ownership protection, copy control, authentication, integrity and many more. Such applications applied to multimedia objects like images, audio and video.

The categories of video object is original [2] or compressed [3] and both can be exploited for watermarking. If video signal is in uncompressed form then spatial or frequency domain base can be used for watermarking purpose but later is most preferred techniques to get the balance tradeoff among all three features of watermarking. Each and every manipulation in the watermarked multimedia object comes under the category of attack. The image processing attacks includes geometric attacks further includes resize, cropping and rotation attacks. In the same category, other attacks are image enhancement attacks as histogram processing, histogram equalization, filtering, noise removal, morphological, contrast enhancement, frame restoration and many more. Other category of attacks are collusion attacks, can have two categories Type-1 and Type-2 attacks. Major important attacks in the same category includes compression attacks, cryptographic attacks, de-noise and scanning attacks. On the other hand, movies objects have

978-1-7281-7016-9/20/$31.00 ©2020 IEEE

their own attacks classified as intentional and unintentional video specific attacks. Some of the attacks in this category are those that not genetic from image watermarking, but exist. The unintentional attacks in video specific attacks are to insert a small video clip as advertisement in the middle of the movie known as frame insertion attacks. Sometimes, a segment of video clip required to cut down. It may be due to film sensor board have objection on some of the scene needed to be deleted before it come into the market. The intentional video specific attacks are frame averaging and frame replacement.

It must be ensuring that the quality of watermarked movie must not be degraded from the minimum threshold known as perceptibility of watermarked video. Another major important feature of video watermarking is payload capacity reflect that how much amount of watermark information can be embedded. All the three conflicting parameters must be designed carefully while embedding the additional information into movie so that there should be balanced tradeoff achieve to watermarked video.

The organization of the paper is as follows. The literature review related to the theme is elaborated in Section 2. The preliminaries of generating the scrambled watermark and features selection of movie clip are defined in Section 3. Section 4 explained the embedding and extraction process. The outcomes of simulation are illustrated in Section 5. Section 6 is set for future work possibilities in the delivered video watermarking technique.

II. Related Work

Rakesh Ahuja et al.[4] described every aspect of digital video watermarking including the applications, features, design principles and the work done by the researchers considering original video only. In this review, the author covers only those papers that exploited the techniques based on spatial domain or frequency domain. Other way to watermark the video by considering the signal compressed or during compression. Further Rakesh Ahuja [5-7] elaborated the work done by those researchers who explored the watermarking method based compressed signal by exploiting MPEG-2, MPEG-4 and H.264 standards. A noteworthy task has already been done for all three kinds of movie data for the preceding two span, yet the issue of sturdiness is a key challenge against image and video processing attacks. Maher et al.[8] elaborated the digital video watermarking scheme. The robustness results are evaluated under geometric attacks on watermarked object. They proposed that the video scenes that do not have motion embedded with low capacity of watermark while video frames having motioned scene were inserted by high payload capacity of watermark by implementing the algorithm in discrete wavelet domain. The watermark embedding scheme is broadly classified into three steps. They selected the central frequencies of the luminance sections of the frames to insert the watermark. Second and final steps illustrated the embedding algorithm scheme and training the wavelet network respectively. The robustness of the scheme is judged by applying various frame specific attacks as frame dropping and frame dropping and also lossy compression attack.

Yang Gaobo [9] implanted the watermark data in every scene of video frame exploiting the wavelet transform domain. The scheme suggested that the encrypted watermark images are segregated into the number of parts that is identical to the sum of scenes in the video sequence.

Yan et al. [10] enlightened the watermarking scheme for video by scene change technique includes support vector machine (SVM). This scheme suggested to train the SVM in some of the frames and rest of the frames are used to insert the watermark through SVM. The sturdiness results are evaluated for compression attack.

Zoran S. Velickovic [11] suggested an algorithm for the security of un-encoded video content from replication by introducing a scrambled watermark in the chrominance channel. The scrambling of the watermark done by a Generalized Multi Stage Arnold Transform map to increase the security. The techniques discrete wavelet transform (DWT) with singular value decomposition (SVD) algorithm in the U component of the YUV color model had been used for embedding the watermark. the quality of the extracted watermark from the channel chrominance is measured by an SSIM index slightly lower quality than that extracted from the luminance channel, but on the other hand, the quality of the protected video is significantly higher.

Yogesh [12] discussed a method to identify the watermark from the distorted video with the use of barrel distortion model. The watermark is extracted by calculating various parameters like correlation, structural similarity index (SSIM) and mean square error (MSE) to notice the accurate watermark signal.

After an exhaustive survey of delivered digital video watermarking technologies based on scene change [13-16] or using transform domain, it is found that none of the scheme is capable enough to claim complete robustness against wide variety of image and video specific attacks while maintaining the good perceptibility and throughput.

In view of all these issues, the proposed paper suggested to implement the watermarking technique for video multimedia objects by considering only motion frames. Since motionless frames are never be a part of watermarking process, therefore such frames will be buffered into the watermarked video without any changes. Due to this, the higher perceptibility is obtained. During the extraction of scrambled watermark, the original video and original watermark are required to be proof for solving the copyright issue. Therefore, the resultant watermarking process for video data will be used for private watermarking applications, where the original objects shall be available to proof the ownership protection.

III. Encryption of Watermark

The aim to encrypt the watermark object is to provide the security of the embedded signal so that even if the malicious user got success to extract it then still, he would not be able to get back the plain text. An encryption mechanism is used to encrypt the binary watermark image. The ciphered image can never by differentiated by human being. An appropriate novel encryption algorithm and key based on host signal are used to scrambled the watermark.

A. Column Transposition Method

The mathematical approach to generate the cryptography keys used to encrypt and decrypt the watermark to be embedded in host object defined in the following manner: -

Key α Size(frame), where Key(Let us say 'K') is the number of elements in the key. where 'Size' is defined in terms of rows and columns of video frame K = C x Size(frame), where the value of 'C' is based on extraction of the feature of the video. it is adjusted in such a way that the count of elements must be a multiple of 16 in order to make computation efficient and easy. The structure of key will be as follows:

K = [16, 1,14, 3 ,12, 5, 10, 7, 8, 9, 6, 11,4, 13,2, 15] (1)

B. *Encryption Algorithm*

Once the size (Row x Column) of the watermark image is calculated, it is resized so that the resultant image is completely divisible by N x N where N $\in SizeofKey$. The original image is partitioned equivalent to the number of elements in the Key. These partitioned image parts are permuted according to the equation (1).

The encryption process rearranges odd number of partitions into the even position and even number of partitions in the odd position, but in chronological order. This process reshuffled entire sixteen parts of the image. The resultant image is transpose to get the intermediate encrypted image. The same process is repeated sixteen times to generate the final cipher image

Fig. 1 represent the original watermark image and the matching jumbled image are represented Fig. 2. It is noticeable that the extraction of unscrambled watermark cannot be done until and unless one knows the encryption key and algorithm.

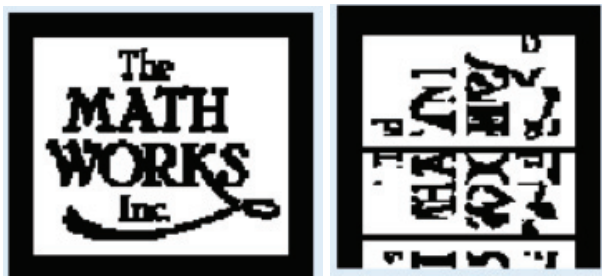

Fig . 1. Original watermark Fig. 2. Scrambled watermark

The encrypted watermark image is partitioned in order to embed each different segmented scrambled image into each different motion frame as per the methods shown below in Equation 2.

$$Count=\left\lfloor \frac{Extracted\ Motion\ Frames}{\frac{No.ofKeyElements}{C}} \right\rfloor \quad (2)$$

For instance, if $Extracted\ Motioned\ frames$ are 14, $the\ count\ of\ elecment\ in\ the\ Key\ 'K'$ are 16 and the value of C is set to 4 then the outcome of $Count$ for segmented encrypted images is 4. The resultant number of segmented scrambled images are defined by Equation (i) in the following Fig. 3.

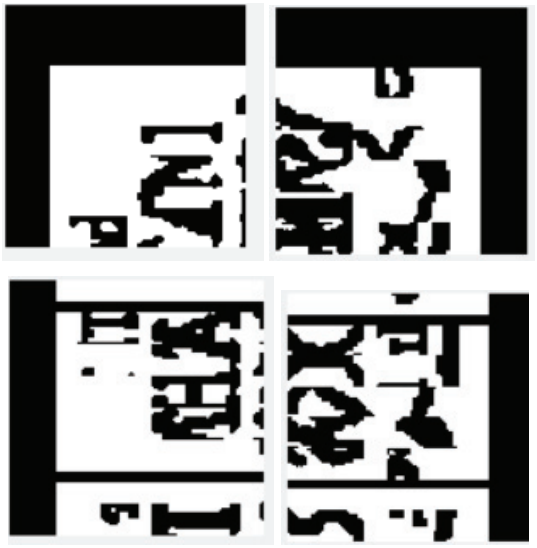

Fig. 3: Parts of scrambled Watermark

C. *Extraction of Motion Frames*

As explored in the previous section, there are lot more limitations are associated video watermarking scheme based on exploiting motionless region or scene-change detection. Therefore, the proposed technique implemented the novel method for video watermarking. The histogram of red component of each frame is utilized to extract the frame considered as motion frame by the following method.

The scheme detected 14 frames as motion frames from the static video Gemini after setting the threshold to 5000. Entire 14 motion frames and the corresponding histogram are shown in the Fig. 4 and Fig 5 respectively.

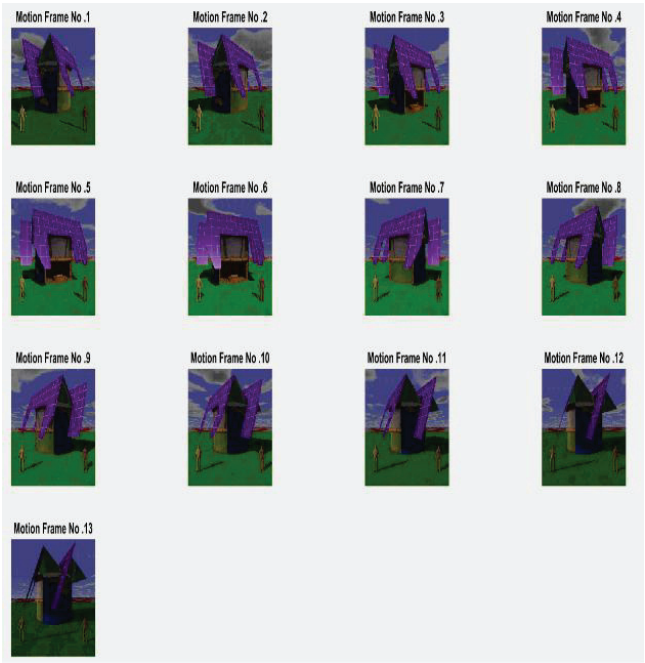

Fig. 4: 14 Motion frames from Gemini

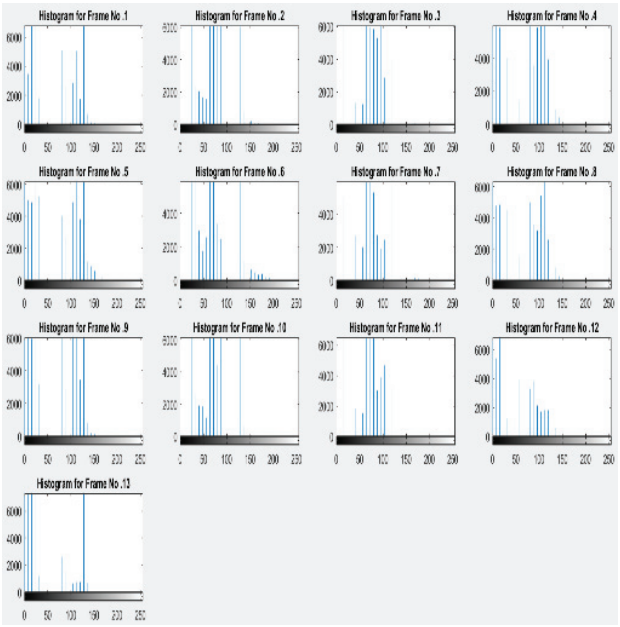

Fig. 5. The Corresponding Histogram

IV. Video Watermarking Process

The proposed watermarking algorithm embedded each segment of encrypted watermark into each different video frame consisting motion with respect to previous frame. Only few frames are watermarked by using this approach, therefore the quality of watermarked video object is maintained. The insertion and extraction algorithms are defined below.

A. Watermark Insertion

Each video frame of 'Gemini' and check whether it is considered to be motion frame based on some predefined process defined in Section 3.2 then the concern frame is chosen for watermark by picking first part of encrypted watermark image otherwise leave this frame without in original form. Now, another frame is checked and repeat the same process. If it is motion frame then chose the next part of encrypted watermark to embed into second motion frame by considering the fact that first part is exhausted in previous motion frame. In this way, all parts are exhausted in all motion frames. If the number of motion frames are greater than the number of partitioned images then the embedded process will start from the scratch to embed the parts of watermark image with remaining motion frames in order to make puzzle for assailant. The motion frame is converted into luminance component 'Y', chrominance blue. components 'Cb' and chrominance red 'Cr' by the Equation 3 :

$$[Y \quad Cb \quad Cr] = [R \quad G \quad B] \begin{bmatrix} 0.299 & 0.596 & 0.212 \\ 0.587 & -0.275 & -0.523 \\ 0.114 & -0.321 & -0.311 \end{bmatrix} \tag{3}$$

Haar wavelet transform (DWT) is applied at two levels at Y. The outcome is to get four different energy subbands named as LL, LH, HL and HH. sub-bands HH is used to extract the used to insert the watermark. low LL and middle energy sub-bands LH and HL are not used for watermarking purpose as they may reduce the excellence of watermarked video. HH sub-band is passes through the DCT function followed by SVD function. Diagonal matrix generated from SVD operation is used to watermark purpose as per the following equation.

$$S_{WTR} = S_A + \mu S_W \tag{4}$$

Where S_A and S_W represents the diagonal matric from SVD operation on DCT image and part of encrypted watermark image and SWTR is the SVD of watermarked frame. The best value of μ obtained is 0.01 by experimenting on the combination of different video and watermarks. A reverse process is applied to generate the watermarked video.

B. Watermark Extraction

Extract two adjacent RGB frames from the watermarked video. If the later frame is a Motion Frame then it is considered that it contains the watermark. Otherwise continue to extract another frame. Convert the RGB frame into Y, Cb, and Cr component. and chrominance components. Discrete wavelet transform(DWT) is applied upto two level to extract the higher energy sub-band (HH) followed by DCT and SVD transformation to generate three matrices as UA, SA and VA. The singular value of the watermark (SW') is obtained by using the following formula.

$$SW' = (SO - Sw)/ \mu \tag{5}$$

where SO and Sw are the singular value of the original motion video frame and watermarked motion video frame respectively. The watermark from the first motion frame from both the video is obtained by the following way.

$$\text{Estimated Watermark} = UW \times SW' \times VW \tag{6}$$

where (UW, VW) ∈ orthogonal matrix of original watermark.The above process is repeated to obtain all the estimated watermark image from entire unique motion frames. Final watermark image is predicated by taking the average from all the estimated watermark image.

V. Simulation Results

Perceptibility and robustness have been checked by simulating various tests for the proposed video watermarking method. The main motive is to extract the embedded watermark from watermarked video by applying different types of nonintentional or intentional attacks. The color static video object Gemini consisting 299 video frame. The size of each video frame is 180 x 720. 120 x 107 is the size of watermark image as copyright information selected for inserting into video Gemini. The main challenge is to measure the perfect perceptibility in video because the amount of distortion and visibility is strongly depends on the video object. However, Peak Signal to Noise Ratio(PSNR) is the measuring tool to get the perceptibility defined below

$$PSNR = 20 \log_{10}(\max_i / \sqrt{MSE}) \tag{7}$$

where

$$MSE = 1/MxN \sum_{i=1}^{M} \sum_{j=1}^{N} ||OF - WF'|| \tag{8}$$

maxi=max (WF (i,j), i and j ranges from 1 to M and 1 to N respectively and MSE is the mean square error between the original frame OF and the watermarked frame WF' . The unit of PSNR is in dB. An example of last original frame and corresponding watermarked frame from the Gemini video shown in Fig 6 a and Fig. 6 b respectively.

Fig. 6 a. Original frame

Fig. 6 b Corresponding from Foreman watermarked frame

The sturdiness is obtained by comparing the watermark extracted and the original watermark between original and extracted watermark to judge the similarities between two defined as

$$NC = \frac{\sum i \sum j . w_{ij} * w'_{ij}}{\sqrt{\sum i \sum j (w_{ij})^2} \sqrt{\sum i \sum j (w'_{ij})^2}} \quad (9)$$

where W_{ij} and W'_{ij} *and* are pixel element of the i^{th} row and j^{th} column of original and extracted watermark respectively. The proposed scheme obtained the high PSNR of 50.88 dB as the minimum accepted value is around 30dB. Further, the original watermark and its four parts are exposed in the Fig 7 and the encrypted watermark at source and received end and decrypted version of watermark are exposed in Fig. 8 and the robustness (NC) obtained is 0.98 with no attack.

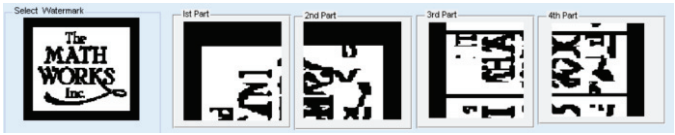

Fig. 7 Original Watermark and all Sub-Parts

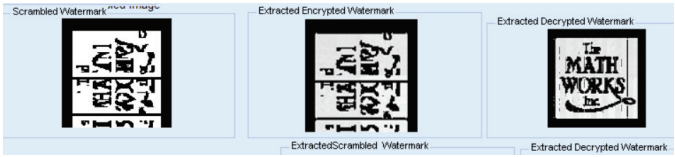

Fig 8 (a) Encrypted watermark at Source End, (b). Extracted Scrambled Watermark , (c). Decrypted Version of The Extracted Watermark

A. Robustness Evaluation

The sturdiness of the proposed theme is conducted by measuring numerous experiments. The properties of video are examined to measure the sturdiness of the proposed scheme. The most notable property of video is its temporal characteristic known as the sequence of video frames. Frame averaging, frame deletions, frame insertion, frame swapping and frame dropping comes under the intentional attacks. Yet, few of the robustness issues are carried from image watermarking. The attacks in this category are image enhancement as adjusting brightness, sharpening, contrast enhancement. Geometric attacks are also inherited from image watermarking. These attacks are cropping, resize and rotatrion of watermarked object. Image processing attacks also includes different noise attacks as *Gaussian noise, Salt and Pepper noise, Poisson noise* and *Speckle noise*. The proposed scheme estimates the resilience of watermark system by covering all above defined attacks. The below mentioned Table I shows that the sturdiness of the proposed scheme.

TABLE I. ROBUSTNESS RESULTS

S.No.	Type of Attack	Sturdiness (NC)
1	Rotation	0.9311
2	Cropping	0.9434
3	Frame Averaging	0.9354
4	Frame swapping	0.9625
5	Frame Replacement (10%)	0.9312
6	Frame Deletion (10%)	0.9165
7	Speckle	0.8728
8	Poisson	0.6312
9	Gaussian	0.8307
10	Salt and Pepper	0.8104
11	Lossy Compression	0.7952

VI. CONCLUSION

The attraction of the proposed theme is to survives the robustness against image processing attacks, video specific attacks and specially compressions attacks. The security of watermark is handled at two level. Before embedding the watermark, first it is encrypted and then partitioned into sub-images to embed in only motion frames. All video frames are not part of embedding algorithm, yet only 4% (13 frames out of 299) are watermarked. Therefore, the quality of watermarked video is highly accepted. There is no viable difference between the original and watermarked video. The resulting watermarking algorithm is perfectly suited for private watermarking application as it is considered that original watermark and original video are available during the extraction process. The future work suggested that the more robustness shall be evaluated for composite attacks, collusion attacks for Type-1 and Type-2, ambiguity attack and the algorithms also design for blind video watermarking where neither original video nor original watermark is available.

REFERENCES

[1] Doerr, G. and Dugelay, J.L., 2003. A guide tour of video watermarking. Signal processing: Image communication, 18(4), pp.263-282.

[2] Li, Qiming, and Ee-Chien Chang. "Zero-knowledge watermark detection resistant to ambiguity attacks." In Proceedings of the 8th workshop on Multimedia and security, pp. 158-163. 2006.

[3] Ahuja Rakesh, S. S. Bedi, 2016. Compressed Domain Based Review on Digital Video Watermarking Techniques. Information Technology of Elixir International Journal, 101, pp. 43622-43633.

[4] Ahuja, R. and Bedi, S.S., 2015. All Aspects of Digital Video Watermarking Under an Umbrella. International Journal of Image, Graphics and Signal Processing, 7(12), p.54.

[5] Ahuja, Rakesh, and S. S. Bedi. "Robust Video Watermarking Scheme Based on Intra-Coding Process in MPEG-2 Style." International Journal of Electrical & Computer Engineering (2088-8708) 7, no. 6 (2017).

[6] Ahuja, Rakesh, and Sarabjeet Singh Bedi. "Video watermarking scheme based on IDR frames using MPEG-2 structure." International Journal of Information and Computer Security 11, no. 6 (2019): 585-603.

[7] Ahuja, Rakesh, and S. S. Bedi. "Copyright protection using blind video watermarking algorithm based on MPEG-2 structure." In International Conference on Computing, Communication & Automation, pp. 1048-1053. IEEE, 2015.

[8] El'Arbi, M., Amar, C.B. and Nicolas, H., 2006, July. Video watermarking based on neural networks. In 2006 IEEE International conference on multimedia and expo (pp. 1577-1580). Ieee.

[9] Gaobo, Y., Xingming, S. and Xiaojing, W., 2006, November. A genetic algorithm based video watermarking in the DWT domain. In 2006 International Conference on Computational Intelligence and Security (Vol. 2, pp. 1209-1212). IEEE.

[10] Yen, S.H., Chang, H.W., Wang, C.J., Wang, P.S. and Chang, M.C., 2008, December. A scene-based video watermarking technique using

SVMs. In 2008 19th International Conference on Pattern Recognition (pp. 1-4). IEEE.

[11] Zoran S. Velickovic, Zoran N. Milivojevic, Marko Z. Velickovic " A secured Digital Video Watermarking in Chrominance Model",IEEE 23rd International Scientific-Professional Conference on Information Technology (IT), 2018.

[12] Yogesh Verma , Manjit Singh , Implementation the Effects of Barrel Distortion in field of Digital Video Watermarking, International Journal of Science, Engineering and Technology Research (IJSETR) Volume 6, Issue 6, ISSN: 2278 -7798, June 2017

[13] Leelavathy, N., Prasad, E.V. and Kumar, S.S., 2012. A scene based video watermarking in discrete multiwavelet domain. International journal of multidisciplinary sciences and engineering, 3(7).

[14] Hampapur, A., Gorkani, M.M., Shu, C.F. and Gupta, A., Virage Inc, 2004. Method for detecting scene changes in a digital video stream. U.S. Patent 6,738,100.

[15] Venugopala, P.S., Sarojadevi, H., Chiplunkar, N.N. and Bhat, V., 2014, January. Video watermarking by adjusting the pixel values and using scene change detection. In 2014 Fifth International Conference on Signal and Image Processing (pp. 259-264). IEEE.

[16] Chan, P.W., Lyu, M.R. and Chin, R.T., 2005. A novel scheme for hybrid digital video watermarking: approach, evaluation and experimentation. IEEE transactions on circuits and systems for video technology, 15(12), pp.1638-1649.