An Efficient Video Watermarking using Spatial Domain and Lab Color Space

Mandeep Kaur
M. Tech Student
Department of Computer Science and Engineering
Sri Guru Granth Sahib World University
Fatehgarh Sahib

Ada
Assistant Professor
Department of Computer Science and Engineering
Sri Guru Granth Sahib World University
Fatehgarh Sahib

ABSTRACT
Video watermarking is the process of embedding watermark in a video. Watermark in a video is embedding by extracting a frame from it and then applying certain techniques. Earlier the conventional techniques of video watermarking like transform domain were used. All the existing transformation techniques have various disadvantage like less robust to additive noise, localization was comparatively poor, not a good quality, less security, higher computation cost, higher frequency rate etc. The need of proposing new technique for video watermarking is to improve the quality and security of watermarked video. In the proposed scheme, lab color space conversion is used. To overcome the disadvantages of the conventional techniques and the security of the system and data compression needs to be improved, PSNR and SSIM should be increased using new technique and the BER should be decreased using this techniques. This proposed technique is considered to be better and the efficient than the traditional techniques of watermarking.

Gernal Terms
Video watermarking.

Keywords
Video Watermarking, Watermark, Transformation Techniques, Lab Color Space, Security.

1. INTRODUCTION
Digital data are break down across high speed networks like the internet and World Wide Web. This data is simplicity accessible for sharing. The ease of reproduction and manipulation of digital documents creates problems for authorized parties that wish to prevent illegal use of such document [1]. Digital watermarking has appeared as a new area of research in an essay to prevent illegal copying and duplication. Digital watermarking is used to secrete the information or data inside a signal, which cannot be simply extracted by the third party. Digital watermarking types are:

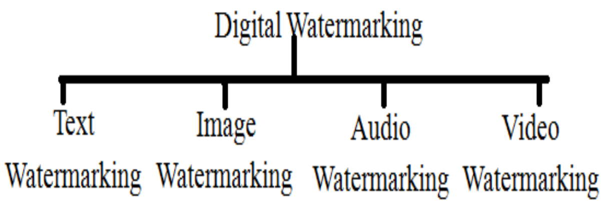

Fig1: Types of Digital Watermarking [18].

1.1 Text Watermarking
In the text watermarking, watermark is used as a watermark text image. It can be no visible or visible. It can be applied in the design and background of perspective of the images [18].

1.2 Audio Watermarking
In audio watermarking, additional signal is inserted or embedded as a watermark into the audio signal [18].

1.3 Image Watermarking
In the image watermarking, watermark is inserted or embedded none visibly in the host image so that watermark can be extracted later for the evidence of rightful ownership [18].

1.4 Video Watermarking
Video watermarking is distinct from image watermarking, because another data are available here that allows information to be more redundantly and reliably inserted. Digital video is a collection of consecutive still images. Video watermarking approaches can be classified into two main parts based on the method of hiding watermark bits in the host video [3]. The video watermarking two parts are: one in which inserting and detection of watermark are performed by just manipulating the pixel intensity values of the video frame. Second alter spatial pixel values of the host video according to a pre-determined transform and are more robust than spatial domain techniques since they separate the watermark in the spatial domain of the video frame making it difficult to delete the watermark through malicious attacks like cropping, rotations and geometrical attacks [4]. Existing video watermarking techniques are divided into different parts as shown in Fig.

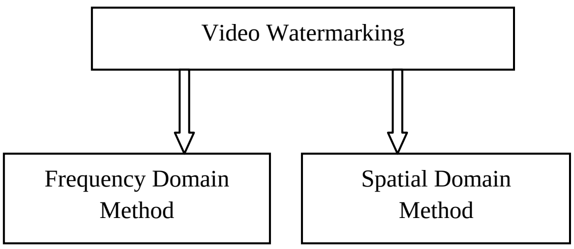

Fig2: Video Watermarking Techniques [4].

1.4.1 Frequency Domain Watermarking-
Most of watermarking techniques the watermark will be embedded or inserted into the frequency domain instead of the spatial domain for the robustness of the watermarking performance. Discrete Cosine Transformation (DCT), Discrete Fourier Transformation (DFT) and Discrete Wavelet

Transformation (DWT) are the three important types of data transformation in this area [5].

1.4.2 Spatial Domain Watermarking

The spatial domain watermarking techniques inserted the watermark by change the pixel values of the host image/video directly. Watermarking in spatial domain determine as a simplex and low complexity process and usually is completed in the luminance component and color component. Different watermarking processes in the spatial domain are, least significant bit modification (LSB), Correlation based techniques [6].

1.5 Video Watermarking Using Lab Color Space

Lab color space is a 3-axis color system with attribute or dimensions *L* for lightness and ***a*** and ***b*** for the color attributes or dimensions. Working with the Lab color space related all of colors in the spectrum, as well as colors outside of human seeing. The Lab color space is the most exact means of defining color and is device independent. This correct and portability makes it eligible in a number of different industries such as printing, automotive, and plastics. Although the Lab color space is the most correct projection of color, it is not the most commonly used. Lab color is usually converted to less exact color spaces, such as RGB and CYMK, because computer monitors and printers use either three or four colors to define images. One of the most important dimension of the L*a*b*-model is device independence. This means that the colors are represented independent of their nature of creation or the device they are displayed on. The lightness, L^*, define the darkest black at $L^* = 0$, and the brightest white at $L^* = 100$. The color channels, a^* and b^*, will define true neutral gray values at $a^* = 0$ and $b^* = 0$ [7].

2. METHODOLOGY

The proposed methodology is divided into two sections. One is the embedding of the data into the video and other section is the extraction of data from the video.

2.1 Methodology of the Data Embedding Process

Step1: Initially the video is loaded from the given set of video. In this video the data is hide that is send to the receiver.

Step2: After selection of the video, next step is to extract the frames of the video. These frames are extracted in order to hide information.

Step3: Next step after the extraction of frames is the conversion of the extracted frames into Lab color space.

Step4: A watermarked image is loaded that is hided in the video, after the selection of the watermarked image. An encryption key is entering for encryption of data. By using this watermarked image will be encrypted and security of the watermarked is increased.

Step5: In this step the watermarked image is hided in the extracted frame of the video by using data hiding process.

Step6: After this the lab color space image is converted into RGB, the image is converted into RGB format and after that it is send and the video is reconstructed and is send to the receiver.

Step7: Finally the calculations of the performance parameters are done. These parameters will describe the efficiency of the system.

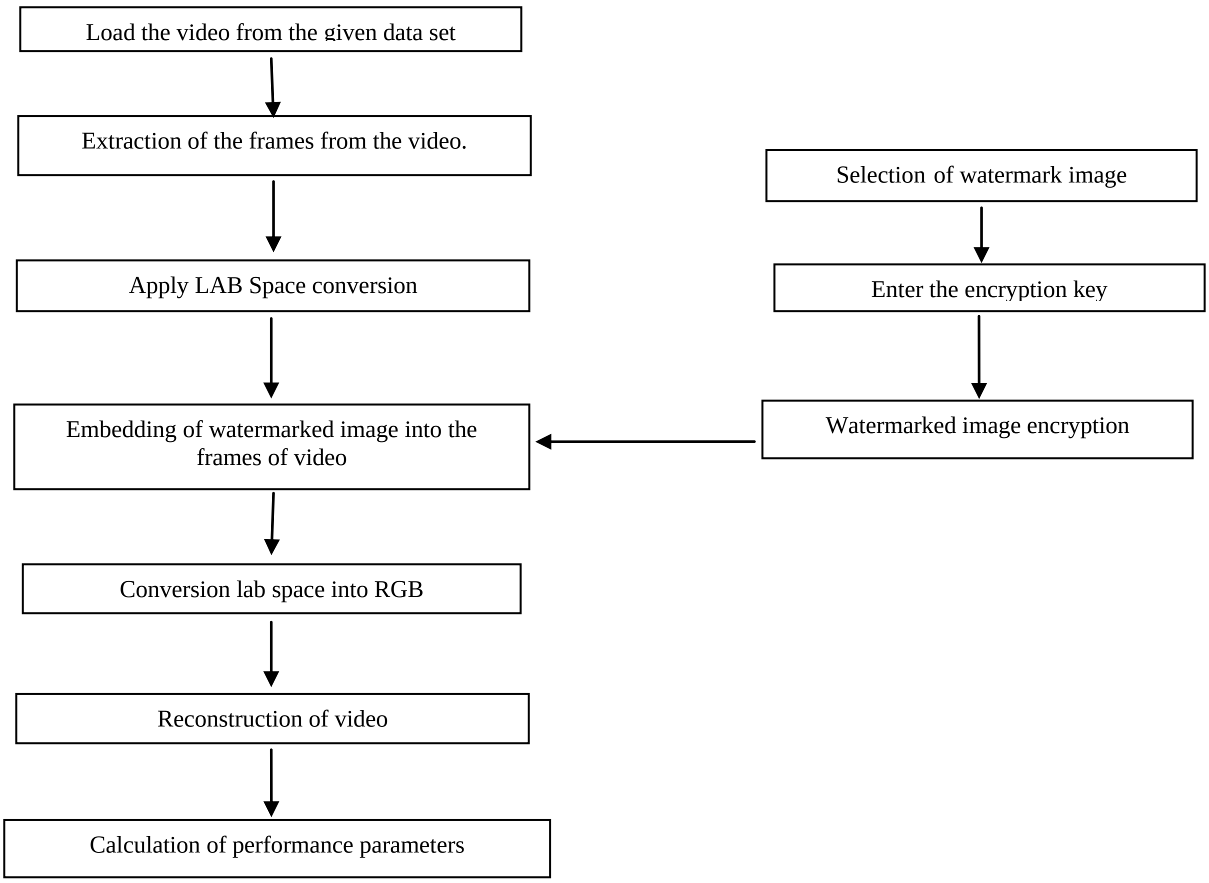

Fig3: Data Embedding.

2.2 Methodology of the Data Extracting Process

Step1: For the extraction of the data the encrypted video is loaded in which the data is hiding by the sender.

Step2: After selection of the video, next step is to extract the frames of the video. These frames are extracted contain the hidden information.

Step3: Next step after the extraction of frames is the conversion of the extracted frames into lab color space.

Step4: On other side the data encrypted video is selected and the extraction of the frame is done, that are further converted into the Lab color space.

Step5: In this step the data extraction is done. By doing the frames in which the information is hided are obtained.

Step6: Finally the watermark image is recovered that was send by the user.

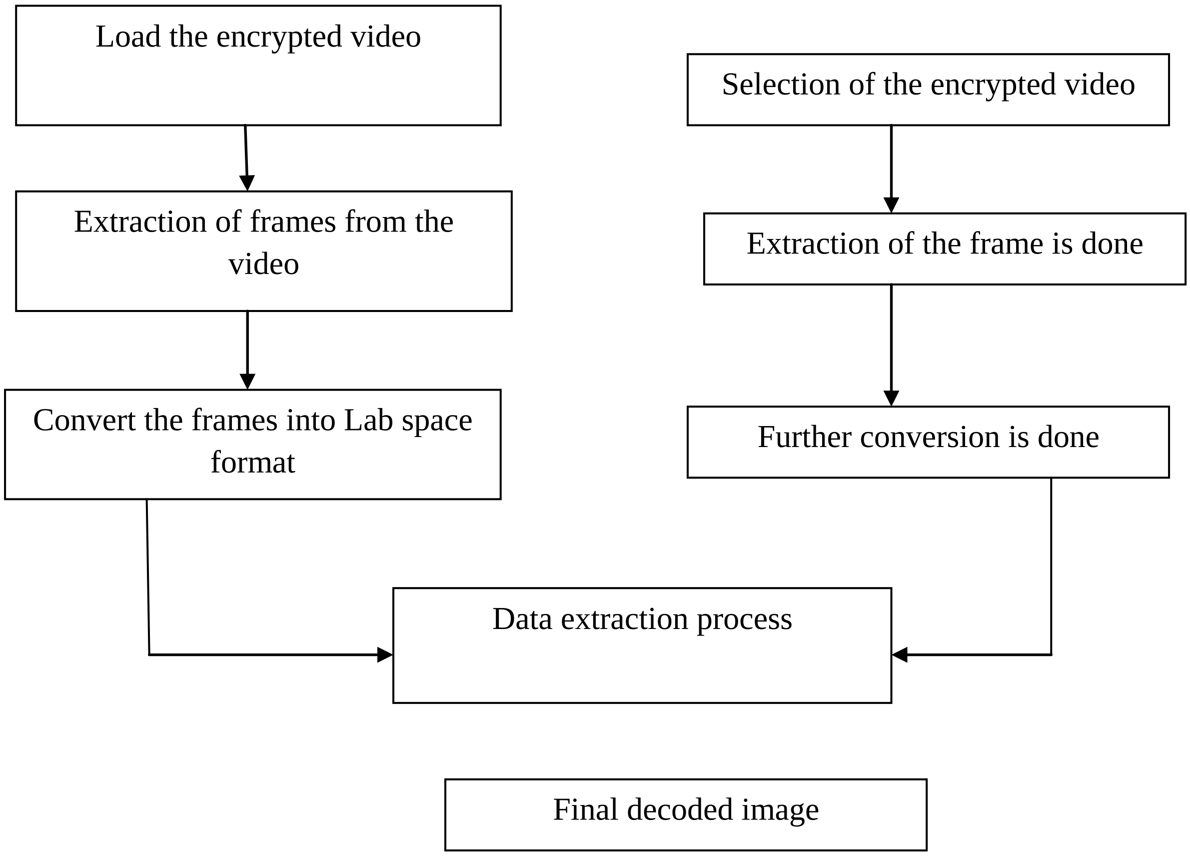

Fig4: Data Extraction

3 IMPLEMENTATION

The proposed work is divided into two sections. One is the embedding of the data into the video and other section is the extraction of data from the video.

3.2 Data Embedding Process

Step1: Initially the video is loaded from the given set of video. In this video the data is hide that is send to the receiver.

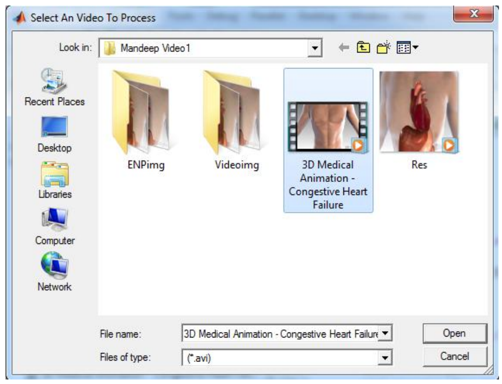

Fig5: Select a Video to Process

Step2: After selection of the video, next step is to extract the frames of the video. These frames are extracted in order to hide information.

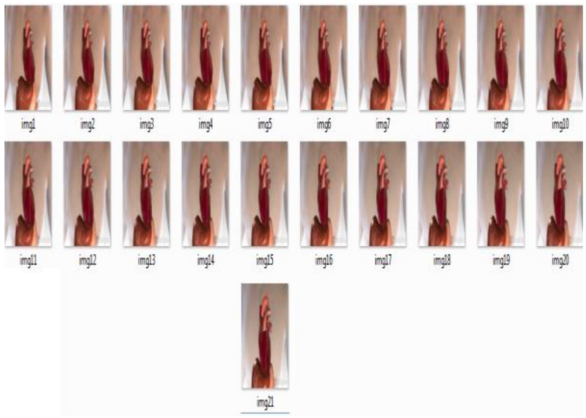

Fig6: Extracted Frames

Step3: Next step after the extraction of frames is the conversion of the extracted frames into Lab color space. It will describe a video watermarking technique which is based spatial domain, such as lab color space. In this section, introduce the transformation of video watermarking technique.

RGB to LAB Conversion: Compost images in MATLAB from RGB to LAB color space. The RGB color space lies of all possible colors that can be made by the mixture of red, green, and blue light. It's a democratic model in photography, television, and computer graphics. RGB2Lab takes red, green, and blue array matrix, or a single M x N x 3 image, and move an image in the LAB color space. RGB values can be lies between 0 and 1 or between 0 and 255. Values for L are lies in range [0,100] while a and b are about in the range [-110,110].

Syntax

[L, a, b] = RGB2Lab(R, G, B)
[L, a, b] = RGB2Lab(I1)
I2 = RGB2Lab(R, G, B)
I2 = RGB2Lab(I1)

Step4: A watermarked image is loaded that is hided in the video, after the selection of the watermarked image. An encryption key is entering for encryption of data. By using this watermarked image will be encrypted and security of the watermarked is increased.

Fig7: Selected Watermark Image

Step5: In this step the watermarked image is hided in the extracted frame of the video by using data hiding process.

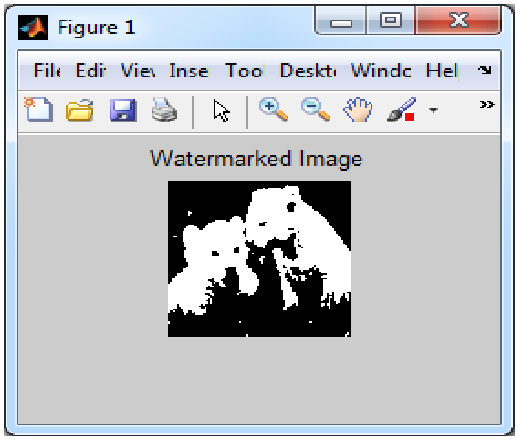

Fig8: Embedded Watermarked Images

Step6: After this the lab color space image is converted into RGB, the image is converted into RGB format and after that it is send and the video is reconstructed and is send to the receiver.

LAB to RGB Conversion: Compost LAB images in MATLAB to RGB. L*ab is defined by lightness and the color-opponent attributes a and b, which are depends on the compressed Xyz color space coordinates. Lab is expressly notable for its use in delta-e calculations. RGB values may be belonging in the range from 0 to 255 or from 0 to 1. LAB values range as follows: L values lies between 0 and 100, and a and b values lie between -110 and 110. Output from Lab2RGB is given between 0 and 1. The input and output can be 3 different matrices.

Syntax

[R, G, B] = Lab2RGB (L, a, b)
[R, G, B] = Lab2RGB(I1)
I2 = Lab2RGB(L, a, b)
I2 = Lab2RGB(I1)

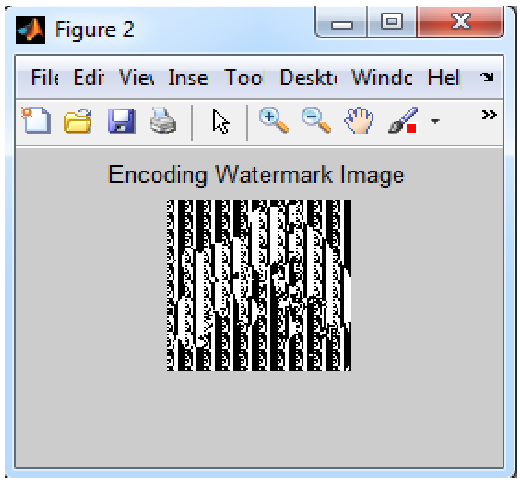

Fig9: Encoding Watermark Image

Step7: Finally the calculations of the performance parameters are done. These parameters will describe the efficiency of the system.

3.3 Data Extracting Process

Step1: For the extraction of the data the encrypted video is loaded in which the data is hiding by the sender.

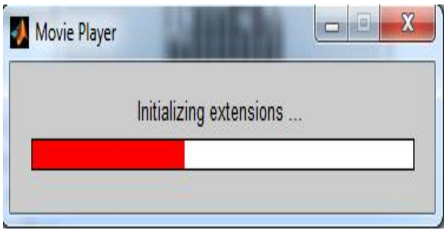

Fig10: Encrypted Video is loaded.

Step2: After selection of the video, next step is to extract the frames of the video. These frames are extracted contain the hidden information.

Fig11: Extracted Frame

Step3: Next step after the extraction of frames is the conversion of the extracted frames into lab color space.

Step4: On other side the encrypted video is selected and the extraction of the frame is done, that are further converted into the Lab color space.

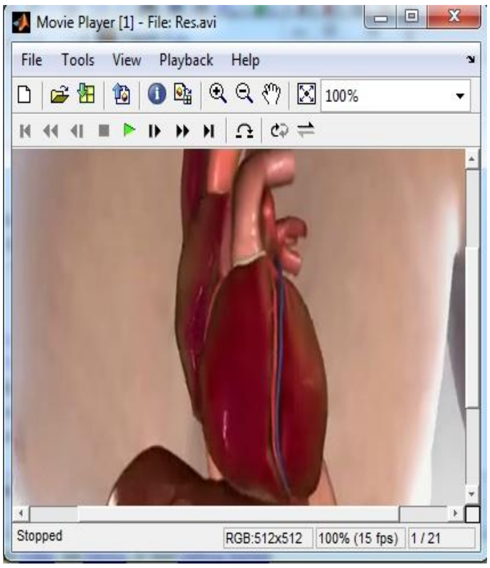

Fig12: Encrypted Video.

Step5: In this step the data extraction is done. By doing the frames in which the information is hided are obtained.

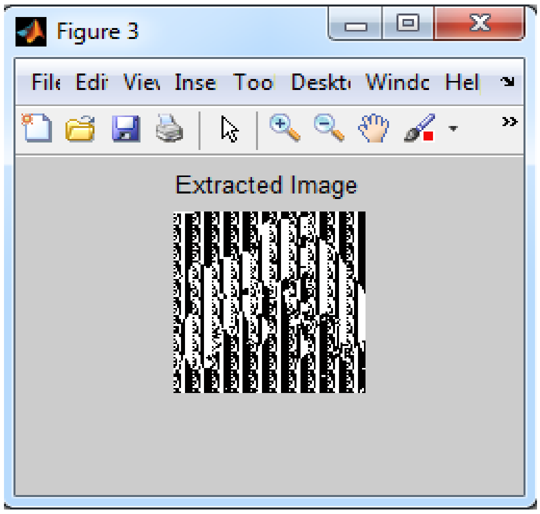

Fig13: Watermark Extracted Images.

Step6: Finally the watermark image is recovered that was send by the user.

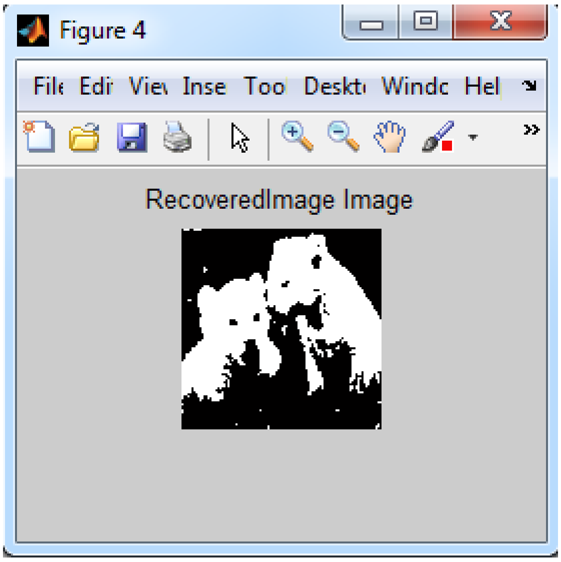

Fig14: Recovered Image

3.4 Performance Analysis

Video watermarking quality evaluation parameters are as follows:

To evaluate the performance of the proposed scheme, we used video with AVI format. This video has least 100 frames which are available. Video watermarking used for evaluation of the proposed scheme. The proposed scheme is assess from the watermark imperceptibility and robustness points of view. After selection of the video, is to extract the frames of the video. These frames are extracted contain the hidden information. Video frames are:

Fig15: Img100.

Fig16: Img101.

Fig17: Img102.

Fig18: Img103.

Fig19: Img104.

Four kinds of parameters are defined as follows:

1) **Mean Square Error:** The Mean Square Error (MSE) is the error metrics used to analyze image compression quality. The MSE express the cumulative squared error between the compressed and the original image.

D = abs (double (imge new)-double (imge org)) ^2
MSE = sum (D (:)) /numel (imge new)

Table1: The Results of the Statistical MSE Parameter

Frames	Proposed MSE
Fig4.1	0.5417
Fig4.2	0.5446
Fig4.3	0.5475
Fig4.4	0.5525
Fig4.5	0.5578

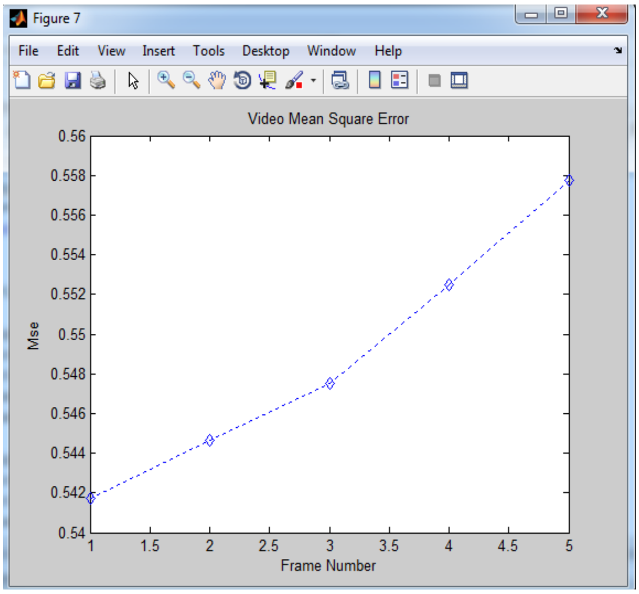

Fig20: Mean Square Error

The above graph shows that the Mean Square Error (MSE) parameter calculated because the value of MSE is used for the calculation in PSNR.

2) **PSNR: Peak Signal to Noise Ratio:** The Peak Signal to Noise Ratio (PSNR) is the error metrics used to analyze image compression quality. Whereas PSNR define a measure of the peak error.

PSNR= 10*log10 (Q*Q/MSE)

Table2: Compare the Results of the Old and ProposedPSNR Parameter

Frames	Old PSNR	Proposed PSNR
Fig4.1	33.5200	50.8269
Fig4.2	33.6600	50.8038
Fig4.3	33.0400	50.7810
Fig4.4	33.6100	50.7417
Fig4.5	33.0400	50.7004

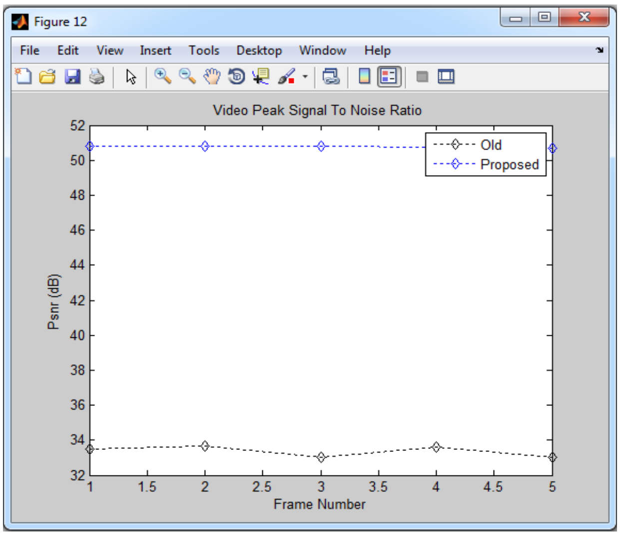

Fig21: Video Peak Signal to Noise Ratio.

In this graph define the Peak Signal to Noise Ratio (PSNR) parameter values are compared with old values. In this graph show the less peak error and less noise ratio.

3) **SSIM: Structural Similarity Index:** The SSIM is a method for indicate the perceived quality of digital television and cinematic images, as well as other kinds of digital images and videos.

SSIM = ((2*mu1_mu2 + C1) *(2*sigma12 + C2)) /((mu1_sq + mu2_sq + C1) *(sigma1_sq + sigma2_sq + C2))

Table3: Compare the Results of the Old and Proposed SSIM Parameter

Frames	Old SSIM	Proposed SSIM
Fig4.1	0.8400	0.9991
Fig4.2	0.8450	0.9991
Fig4.3	0.8190	0.9991
Fig4.4	0.8450	0.9991
Fig4.5	0.8190	0.9990

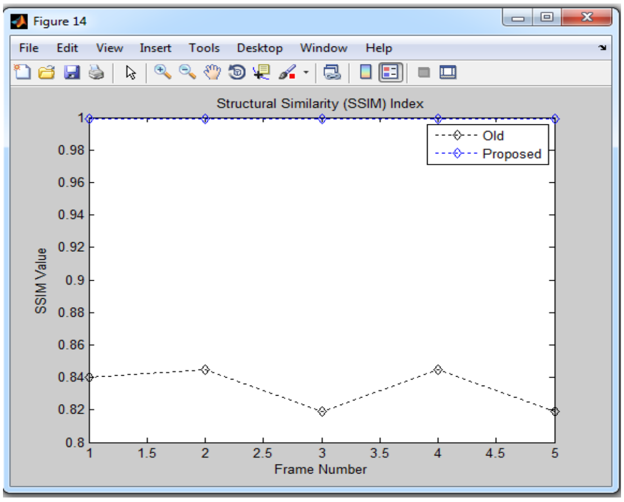

Fig22: Structural Similarity Index.

In this graph increase the Structural Similarity Index (SSIM) parameter values as compared to old values. Then also provide a good quality of the watermark image.

4) **BER: Bit Error Rate:** BER is a key parameter that is used in evaluates systems that transmit digital data from one location to another. The rate at which errors occur in the sending of digital data. BER is used to quantify a channel pack data by counting the rate of errors in a data string.

Table4: Compare the Results of the Old and Proposed BER Parameter

Frames	Old BER	Proposed BER
Fig4.1	0.0080	0.0020
Fig4.2	0.0070	0.0020
Fig4.3	0.0080	0.0020
Fig4.4	0.0090	0.0020
Fig4.5	0.0060	0.0020

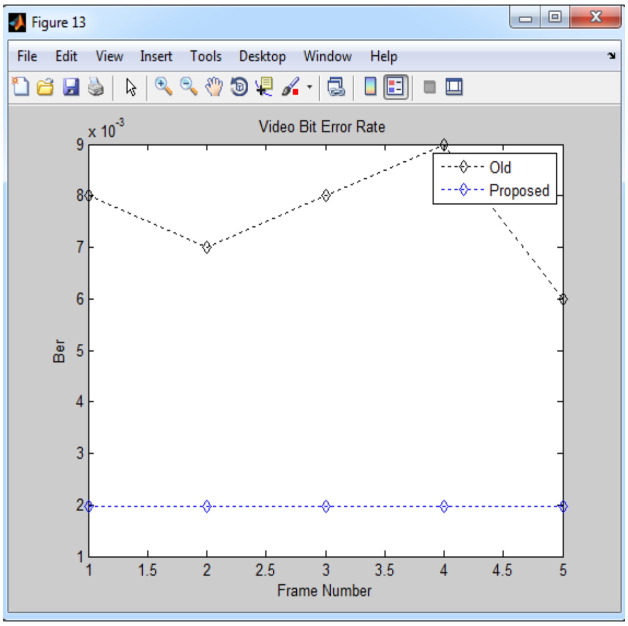

Fig23: Video Bit Error Rate.

In this graph describes the old and proposed Bit Error Rate (BER) parameter values. It will decrease the BER parameter values as compared to old values.

4 CONCLUSIONS

Watermarking is a technique of embedding image or data in an image, video or audio for securing the data that is hidden or for authentication purposes. Traditional algorithm may have been proposed for the video watermarking but the results achieved were not efficient. So in this proposed method for increasing the security of the watermark, PSNR and SSIM should be increased using new technique and the BER should be decreased using proposed techniques, the encryption of the watermark is done before embedding it into the video and the frames of the video are converted into lab color space format before the data is hided. The experimental results show fairly good watermark imperceptibility since the obtained PSNR values are near to 50 db and the SSIM is close up to 1, the BERs of the proposed scheme are smaller than 0.002. From results it is concluded that this method better than the traditional method of watermarking as the security of the watermark is increased.

5 FUTURE WORK

For the results obtained it is analyzed that the proposed technique is better than the traditional techniques. The security of the watermarked is increased by encrypting the data before embedding into video. In future this work can be further enhanced by increasing the security of the watermarking process so that it is not access by any unauthorized user. Also various other data hiding technique can be used for embedding the data into the video.

6 REFERENCES

[1] Ekta Miglani, Sachin Gupta, "Digital Watermarking Methodologies-A Survey", International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), 2014, Volume 4, Issue 5, pp 826-832.

[2] Munesh Chandra, Shikha Pandey, Rama Chaudhary, "Digital watermarking technique for protecting digital images", Computer Science and Information Technology

(ICCSIT), 2010 3rd IEEE International Conference, Volume 7, pp 226 – 233.

[3] Dr.V.Seenivasagam, "A Survey on Video Watermarking and Its Applications", International Journal of Engineering Research and Applications (IJERA), 2014, Volume 4, Issue 12, pp 39-44.

[4] Anumol Joseph, K. Anusudha, "Robust watermarking based on DWT and SVD", International Journal of Signal & Image Processing, 2013, Volume 1, Issue 1.

[5] Manoj Kumar, Mrs. Dolley Shukla, "Review of Video Watermarking Techniques", IJIRST–International Journal for Innovative Research in Science & Technology, 2013, Volume 1, Issue 8.

[6] Dr. M. Madhavi Latha, Kesavan Gopal, "Watermarking of digital Video Stream for Source Authentication", International Journal of Computer Science Issues, 2010, Volume 7, Issue 4.

[7] DibyaJyoti Bora, Anil Kumar Gupta, Fayaz Ahmad Khan, "Comparing the Performance of L*A*B* and HSV Color Spaces with Respect to Color Image Segmentation", International Journal of Emerging Technology and Advanced Engineering, 2015, Volume 2, pp 192.

[8] Antonio Cedillo-Hernandez, Manuel Cedillo-Hernandez, Mireya Garcia-Vazquez**,** "Transcoding resilient video watermark scheme based on spatio-temporal HVS and DCT", ELSEVIER, 2014, Volume 97, pp 40–54.

[9] Bernd Girod, Jonathan K. Su, Frank Hartung, "Digital Watermarking of Text, Image, and Video Documents", ELSEVIER, 1998, Volume 22, pp 6.

[10] Munesh Chandra, Shikha Pandey, Rama Chaudhary, "Digital watermarking technique for protecting digital images", Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference, Volume 7, pp 226 – 233.

[11] Manjit Thapa, Dr. Sandeep Kumar Sood, A.P Meenakshi Sharma, "Digital Image Watermarking Technique Based on Different Attacks", (IJACSA) International Journal of Advanced Computer Science and Applications, 2010, Volume 2, No. 4, pp 14 -19.

[12] Puneet Kr Sharma, "Analysis of image watermarking using least significant bit algorithm", International Journal of Information Sciences and Techniques (IJIST), 2012, Volume 2, No.4, pp 95 -101.

[13] G. G. Chiddarwar, GV Mane, "Review Paper on Video watermarking Techniques", International Journal of Scientific and Research Publications, 2013, Volume 3, Issue 4.

[14] Loganathan Agilandeeswar, Kumaravel Muralibabu, "A robust video watermarking algorithm for content authentication using Discrete Wavelets Transform (DWT) and Singular Value Decomposition (SVD)", International Journal of Security and Its Applications, 2013, Volume 4, pp 2.

[15] Radhika v. Totla, K.S.Bapat, "Comparative Analysis of Watermarking in Digital Images Using DCT & DWT", International Journal of Scientific and Research Publications, 2013, Volume 2, pp 1-4.

[16] R.J.Iswarya, R.Poornima, "An overview of digital image steganography", International Journal of Computer Science & Engineering Survey (IJCSES), 2013, Volume 4, Issue 1.

[17] Mrs. Rashmi Soni, Prof.M.K.Gupta, "Digital Watermarking of Wavelet Transforms Based on Coding and Decoding Techniques", International Journal of Computer Science and Mobile Computing (IJCSMC), 2014, Volume 3, Issue 3, pp 1045 – 1051.

[18] Ekta Miglani, "Digital Watermarking Methodologies - A Survey", International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), 2014, Volume 4, Issue 5, pp 826-832.

[19] Pawan Singh Shekhawat, Narendar Singh Yadav, "Non Blind DWT Based Multiplicative SVD Watermarking Algorithm", International Journal for Scientific Research & Development (IJSRD), 2014, Volume 3, Issue 03, pp 1844-1848.

[20] De Li, DY Jiang, JW Kim, "Robust Adaptive Video Watermarking Algorithm based on Dual Transform Domains", International Journal of Multimedia and Ubiquitous Engineering, 2014, Volume 9, No.1, pp 391-402.

[21] Lianjie Dong, "A blind digital watermarking algorithm based on DWT", Journal of Chemical and Pharmaceutical Research (JOCPR), 2014, Volume 6, Issue 3, pp 78-89.

[22] [22]Mr. Jagtap. D. V, Mr. M. M. Mukhedkar, "A Secure Data Transmission Scheme Based on Digital Watermarking (Image + Text)", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), 2014, Volume 3, Issue 8, pp 2713-2716.

[23] Mundher, Myasar; Muhamad, Dzulkifli; Rehman, Amjad; Saba, Tanzila; Kausar, Firdous, "Digital Watermarking for Images Security using Discrete Slantlet Transform", Appl. Math. Inf. Sci. 8, 2014, No. 6, pp 2823-2830.

[24] Dong, L., & Wang, R., "A blind digital watermarking algorithm based on DWT", Journal of Chemical and Pharmaceutical Research, 6 (3): 78-89. Journal of Chemical and Pharmaceutical Research, 6(3), 2014, pp 78-89.

[25] Preeti Parashar, RK Singh, "A Survey: Digital Image Watermarking Techniques", International Journal of Signal Processing, Image Processing and Pattern Recognition, 2014, Volume 7, No. 6, pp 111-124.

[26] Zhu Yuefeng, Lin Li, "Digital image watermarking algorithms based on dual transform domain and self-recovery", International Journal on Smart Sensing and Intelligent Systems, 2015, Volume 8, No. 1, pp 199- 219.