Application of Crypto-Video Watermarking Technique to Improve Robustness and Imperceptibiltiy of Secret Data

M. A. Gangarde
Department of Electronics Engineering
Bharati Vidyapeeth Deemed University College of Engineering, Pune, India
maheshgangarde@yahoo.co.in

J. S. Chitode
Department of Electronics Engineering
Bharati Vidyapeeth Deemed University College of Engineering, Pune, India
j.chitode@gmail.com

Abstract – In this paper we have proposed novel and innovative Video Watermarking using Pixel Location Based Technique (PLBT) to improve the robustness and imperceptibility of secret data. We have located the pixel values of selected frames of watermarked video with the obtained pixel values of secret watermark image and locate the respective offset values of selected frames of watermarked video as a secret key. Through different types of attacks on watermarked video during transmission, we have demonstrated that original and watermarked video are exactly identical to each other without any loss of information. The simulation and the comparisons results confirmed the improvement in robustness and imperceptibility of hidden watermarked secret data as compare to any other existing techniques.

Index Terms – PLBT, Watermark Video, Robustness, Security, Attacks

1. Introduction

The main aim of any watermarking technique is for copyright protection and authentication. With today's expanding development in digital communication using internet and many multimedia tools like Twitter, YouTube and Facebook for any type of watermarking technique security of watermark data, authentication, imperceptibility and robustness are the major issues. When such videos are transmitter to receiver the major concern are its security and authentication. For protecting the secret data during digital transmission, it is always better to develop information security model for any multimedia tools. Due to such requirement of multimedia tools, watermarking technique is the better solution for these issues. The suggested video watermarking technique is use for digital communication to enhance the data protection and to improve the quality of original video and watermarked video. In this method pixels locations of watermark image into selected frame of original video are mapped. The amount of pixel location values are replaced directly to the pixel values matched in R, G, B planes. The LSB method proposed by Qingtang Su et al. [3] the changed every LSB values in binary word of all possible pixel values. This brings a significant amount of quality degradation which provides poor parameter results. In the suggested technique, we have minimized the changes in the pixel values by applying different frames of video using pixel location based technique. It is observed from obtained result that there is no degradation in quality of original and watermarked video.

2. Related Work

A. Kunhu et al. in 2016 have developed DCT (Discrete Cosine Transform) and DWT (Discrete Wavelet Transform) based hybrid algorithm which convert three bit index table into color watermark logo for watermarking technique. Then 2-level wavelet decomposition method is applied to the selected channel to a particular band which divided into 8x8 blocks and DCT is applied. Then, the location of same coefficients is selected for hiding the secret watermark data [1]. A spread spectrum technique for multimedia watermark is proposed by I. J. Cox where the watermark is allowed to spread over the whole image spectrum and the modulation is done by the pseudo random sequence. The watermark is retrieved by passing through high pass filter followed by correlation method which improves the robustness [2]. In 2011, S. Patel et al. justified a transform domain watermarking scheme, where the host signal is transformed into frequency domain before embedding the watermark. The watermark signal is distributed almost over the entire host signal are also used for the concealing secret watermark data [3]. In DWT technique, initially, the splitting of the image into RGB components is done then DWT watermarking is applied on every frames of the host video. The author suggested the main advantage of DWT technique is it ensures the security of watermark data and it recovers the exact RGB value without any loss of information [4]. Tabassum et al. in 2012 have introduced a video watermarking scheme based on identical frames extraction using DWT method which reproduces a multi resolution of watermark image. DWT method divides the image into high and low-frequency components till the image is decomposed completely. Generally, the low-frequency components are selected for embedding the watermark. In 3-level DWT, the host video is decomposed into video frames and every identical frame is chosen for 3-level DWT operation which is use for embedding watermark information [5]. In 2012 N. Dey et al. have proposed watermarking scheme in which the video is split into number of frames and decomposed using DWT and DCT is applied to a particular sub band and SVD (Singular Value Decomposition) is applied to the resultant. The same procedure is applied to the watermark image and the host frame is modified according to the watermark [6]. In 2015 Sakthivel S. M. et al. have proposed Pixel Value Searched Algorithm (PVSA) [7] in which pixel by pixel comparison is done between host image and watermark image. They used gray scale image as host image which is distributed in the range of 0 to 255. For every pixel value

978-1-5090-6734-3/17/$31.00 ©2017 IEEE

from watermark image, its same value is searched in cover image. After matching the pixel value position of the cover image is marked as a secret key and repeat same steps for the complete watermark image with threshold value (k). It also presented key size of (2N+2) row position s, in which N = m x n (m indicates row and n indicates column of the watermark image). Y. Lui et al. have presented video watermarking system based on radon transform with frames having highest temporal frequencies to embed the watermark. The watermark embedding technique can be direct or template based in which direct embedding includes embedding by modifying the phase coefficient and magnitudes of DFT while the template based embedding involves the use of templates that depends on the transformation factor [8]. In 2015 Tuan T. Nguyen et al. have described the robust video watermarking technique which is based on Discrete Cosine Transform (DCT) domain with event-odd quantization method. In this technique embedded all bit plane images decomposed from a single watermark image into DCT coefficients of 8x8 blocks from original video. The watermark image is decomposed into bit planes, 8x8 blocks DCT is performed for the luminance component and the random blocks of DCT coefficients are selected for secret key and are arranged in a zigzag manner. The even-odd quantization is applied for reconstructing the watermarked video [9]. N. Deshpande have presented convinced algorithm to hide diverse watermarks in the video frames and examine the robustness of the algorithm by applying the video processing attacks like frame averaging and frame dropping on watermarked video. It also suggested that instead of selecting the entire frames of video, some key frames can be selected for hiding the watermark secret image into original video [10]. R. Ahuja et al. have focused on video watermarking scheme using MPEG-2 coding style which used for the application of copyright protection and it applied various attacks on watermarked video and measured parameters like robustness, perceptibility, embedding capacity along with one more issue 'elapsed time', a serious concern in video watermarking. For testing the performance of video watermarking algorithm and also suggested to apply more video processing attacks like frame insertion, frame deletion, frame averaging and compression attacks [11]. The paper [12] has presented robust video watermarking technique using SURF (Speeded Up Robust Features) system and Discrete Cosine Transform. Robustness of the proposed algorithm is improved by an error-correction code to secure the watermark against bit errors. F. Alenizi et al. have introduced video watermarking method using Discrete Wavelet Transform (DWT) for video authentication and focused on Y-components of the video frames which decomposed by DWT technique where secret watermark image is embedded in one or more resulting sub bands. The simulation result shows the values of average Normalized Correlation (NC) is 0.85 and the Peak Signal to Noise Ratio (PSNR) equal to 45dB. From the simulation results, it is clear that the robustness is very less and quality of the watermarked video is degraded [13]. In 2017, K. J. Kaiser et al. have explained solution for video authentication using watermarking in computer science and information security, cryptology and communications [14]. M. Ghalejughi et al. have proposed video watermarking technique in which chrominance channel of video frames is decomposed into even and odd shares of video frames and selected odd shares for hiding the watermark information [15]. In 2017, K. N. Sowmya et al. gave an overview of video authentication technique and highlights active approaches which is adopted for watermark and digital signature. It also explained limitations of digital signature due to verification process and signature creation depending on application [16].

3. Proposed Information Security model of Robust Video Watermarking Technique using PLBT

The input to the proposed security model is a video of any type of video format. This video is converted into frames and each frame is decomposed into its RGB planes. The watermark image is converted to the grayscale and applied to the block of concealing technique. A secret key is generated from the concealing block based on the matching pixels of the watermark with the video and the output video is generated which is same as the input video. This video and the secret key are applied to the decoding block. The watermark image is reconstructed based on the key and the original video is generated. The complete algorithm of the proposed digital video watermarking technique is illustrated, based on the spatial domain which involves searching the pixel values in cover video matching with the pixel in the watermark image. Based on the match, a location table is constructed which is used as a secret key to provide security and authenticity to the video data as shown in fig. 1.

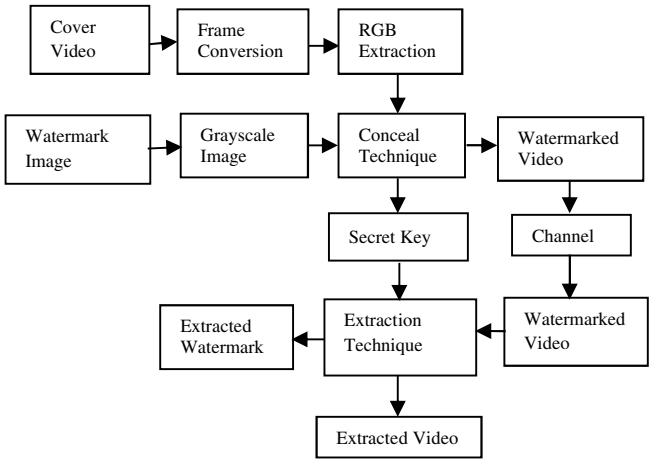

Fig.1 Block diagram of proposed robust video watermarking technique

3.1 Data hiding steps for PLBT

We have obtained the pixel values of watermark image and selected frames of cover video using PLBT algorithm. The cover video is in the RGB format consisting of three planes and the watermark image is in the grayscale format where the pixel value ranges from 0 to 255. We have embedded gray pixel values in R plane of selected frames of color video.

a. *Embedding steps*:

i. Obtain the cover video with RGB values.
ii. Read the cover video and the watermark secret image.
iii. Convert the watermark image to gray scale.
iv. Consider the embedding frame.

v. Consider the first pixel value of the watermark image and search its matching value in the embedding frame.
vi. If the match is found in the cover video frame, store the location of the pixel in the secret key structure.
vii. If the value is not matched then increment or decrement the pixel value of watermark by 1 up to threshold value.
viii. Now find the match of the location of the pixel value, find the difference between the pixel values and store it in key structure.
ix. Converted into all the matching pixel locations separately for R, G, and B planes.
x. The above steps are repeated until the entire pixels of the watermark and update the key structure accordingly.
xi. The output will be the watermarked video which is same as the cover video with the key structure.

b. *Extraction Steps*:

i. Read the watermarked video.
ii. Based on the secret key structure, apply the reverse process to obtain the pixel values of secret watermark image..
iii. Reconstruct the watermark secret image from the values obtained from the secret key.

The embedding frame can be predicted by evaluating the PSNR for all frames with respect to watermark secret image. The frame, for which the maximum PSNR is found among all video frames, is selected for embedding the watermark. The above proposed algorithm is presented with an example frame of cover video of size 8x8 and watermark image of size 4x4 in fig. 2. The fig. 2(a) is the cover frame of the size 4x4 and fig. 2(b) is the watermark image. The first two positions of the secret key structure gives the value of size of secret watermark image and three positions required for locating each pixel of watermark image. For example the first pixel value 168 of watermark image is taken and its value is searched in the cover frame, a match was found in the location (1, 1) which is stored in secret key and the difference between the pixel value of cover frame and pixel value of watermark image i.e. 0 in this case it is stored in secret key as shown in fig. 2(c). In this way the secret key structure is generated in concealing phase and reverse process applied by using same secret key to reconstruct the watermark secret image.

168	53	183	127	27	196	30	51
211	65	172	79	73	56	44	21
45	84	32	243	188	158	159	19
212	199	16	212	28	36	97	33
12	122	196	120	1	88	212	235
56	98	55	61	8	66	45	78
129	150	199	211	48	126	33	57
92	95	11	8	54	38	77	32

a.

168	90	123	79
8	126	78	66
48	196	33	211
52	39	51	100

b.

4	4	1	1	0	8	1	2	5	2	-1	2	4	0	-	-	-

c.

Fig.2 (a) Cover video frame size (8x8) (b) Watermark image of size (4x4) (c) Secret key structure of size (3K+2)
Where K= number of pixel in watermark image

4. Key security parameters and its importance

4.1 Mean Squared Error (MSE)

The mean squared error is the average of the square of the errors or distortions. The squaring is done so that negative values do not cancel positive values [4, 10] as shown in Eq. (1)

$$\mathrm{MSE} = \frac{1}{N}\sum_{i=1}^{N}(x_i - y_i)^2 \quad (1)$$

Where, x_i is the original signal, y_i is the distorted signal; N is the total number of pixels.

4.2 Peak Signal to Noise Ratio (PSNR)

Peak Signal to Noise Ratio (PSNR) is a ratio of the maximum power of a signal to the corrupting noise. PSNR is usually expressed in terms of the logarithmic decibel scale [1, 4]. It is totally dependent on the numeric value and is represented as shown in Eq. (2).

$$\mathrm{PSNR} = 10\log_{10}\left(\frac{\mathrm{MAX}^2}{\mathrm{MSE}}\right) \quad (2)$$

Where, MAX is the maximum possible pixel value in image, MSE is the mean square error.

4.3 Structural Similarity Index Module (SSIM)

Structural similarity index module (SSIM) is a perception base model. It is the measure of similarity between two images [4, 9] as shown in Eq. (3).

$$\mathrm{SSIM}(x,y) = \frac{\left(\mu_x\mu_y + C_1\right)\left(\sigma_{xy} + C_2\right)}{\left(\mu_x{}^2 + \mu_y{}^2 + C_1\right)\left(\sigma_x{}^2 + \sigma_y{}^2 + C_2\right)} \quad (3)$$

4.4 Normalized Correlation (NC)

Robustness of the watermarking algorithm is generally expressed in terms Normalized correlation (NC). NC shows the relation between original image and watermark extracted image [4, 12]. It varies from 0 to 1 and is given by the formula as shown in Eq. (4).

$$\mathrm{NC} = \frac{\sum_1^N\sum_1^M w(i,j)w'(i,j)}{\sqrt{\sum_1^N w(i,j)^2}\ \sqrt{\sum_1^M w'(i,j)^2}} \quad (4)$$

Where, N and M represent the total number of pixels in the watermark image w (i, j) and extracted image w′(i, j) respectively.

4.5 Bit Error Rate (BER*)*

Bit Error Rate (BER) also defines the robustness of the algorithm. It is the ratio of error bits to the total number of transmitted bits [15], ranges from 0 to 1 as shown in Eq. (5).

$$BER = \frac{1}{N}\sum_{i=1}^{N}(x_i - y_i) \quad (5)$$

Where, N is the total number of pixels, x_i and y_i represent the original and extracted image respectively.

5. Robustness and Imperceptibility Through Different Types of Attacks

5.1 Gaussian Noise

The most common type of noise is Gaussian noise. The noise that is present within an image can be modeled as the sum of many independent noise sources. Gaussian noise can be used to model the noise present in an image [9, 10].

5.2 Speckle Noise

This noise is caused due to the errors in transmission of the data. The degraded pixels are set to the new maximum value. This noise affects the ultrasound images [10, 11].

5.3 Salt and Pepper Noise

It represents the white and black pixels that occur randomly on images. This noise comes from images when there are fast transients, for example, faulty switching. In salt and pepper noise, the intensity of the pixels varies from the neighbouring pixels [9, 10]

5.4 Frame Cropping

Cropping is a removal of some portion of the image in order to create focus or replace by black or white pixels. Cropping of the image is done by removing some rows or columns in the image and replacing by black or white pixels. It is a kind of lossy operation [11].

5.5 Frame Dropping, Frame Averaging, Frame Swapping

A video sequence consists of a number of frames arranged at the particular frame rate. During the transmission of the video through the channel, the frames can be affected due to some distortions. These distortions can drop the frames of the video this can affect the performance of the algorithm used for the video watermarking. Some distortions can average of the different consecutive frames results in a single frame and constitutes the video which can degrade the performance. Swapping is nothing but interchanging the specific frame of the video with another one [11, 12].

5.6 Contrast Enhancement

Contrast is the difference in color that makes an image distinguishable. This attack adjusts the image intensity values to enhance the contrast of an image [14].

5.7 Histogram Equalization

The histogram is a frequency plot that corresponds to the occurrence of every possible pixel values in that image [14].

6. Simulation Results

The evaluation and validation of the proposed scheme is obtained calculating key performance parameters in terms of imperceptibility, robustness and its response without attack and after attack. We have applied seven various attacks on watermarked video during transmission process and calculate MSE, PSNR, SSIM, NC and BER before embedding and after embedding watermark which are identical to each other hence perceptibility and robustness of video of proposed technique is increased. The video sample of RGB format named 'Dog.mp4' of size 1280x720 consisting of 321 frames using the image 'cs64.png' whose size is 64x64. Fig. 3(a) shows the original cover video or frame of 'Dog.mp4'and fig. 3(b) is watermark secret image with size 64x64 before hiding into video. Fig. 3(c) indicates the effect of watermark after embedding into original video and fig. 3(d) shows extracted secret 'CS64' watermark image.

(a) Cover Video/Frame (b)Watermark Image

(c) Watermarked Video (d)Reconstructed Watermark

Fig. 3 Cover video and watermark secret image

We have calculate PSNR, MSE of frame number 42 using Eq. (1) and Eq. (2), Here the MSE is 0.3335 and the MAX=255,

$$\text{PSNR} = 10\log_{10}\left(\frac{65025}{0.3335}\right)$$

PSNR=52.89dB

For the frame number 42 of the host video PSNR is 52.89 dB, the remaining parameters are displayed in table 1.

Fig. 4 shows the effect of frame cropping, frame swapping, contrast enhancement and histogram equalization attack on video frame. The original .mp4 Dog video of frames 321 of size 741KB displays in fig. 4(a) by the effect of frame cropping attack on frame number 42 with some distortion. Fig. 4(b) indicates the effect of frame swapping attack on video frame. Fig. 4(c) displays the effect of contrast enhancement on watermarked video and the effect of histogram equalization shows in fig. 4(d).

(a) Frame Cropping (b) Frame Swapping

(b) Contrast Enhancement

(d) Histogram Equalization

Fig. 4 Effect of different attacks on video frames

We have applied various types of attacks on watermarked video which listed in table 1 with extracted watermark image. It also shows the same parameters for before attack and proposed system is tested against various attacks such as Gaussian attack, Speckle Noise, Salt and Pepper Noise, Frame cropping, Frame swapping, Contrast enhancement and Histogram equalization. The effect of noise shown in table 1 with different value of variance such as 0.001, 0.002, 0.003 and 0.01 with MSE, PSNR, SSIM, NC and BER, parameters before attack. The PSNR of 52.89 dB shows the good quality of reconstruction of the watermark and the NC value is 1, BER is 0.11 and SSIM is 0.99. Fig. 5 shows the comparison of PSNR values with different variances of three attacks which indicates that PSNR gradually decreases with increase the value of variance. Fig. 5 displays the comparison of PSNR (dB) with different values of variance for attacks like Gaussian attack, Speckle Noise, Salt and Pepper Noise

Table1. Performance evaluation before and after attack

	Variance	Extracted Watermark	MSE	PSNR (dB)	NC	SSIM	BER
Before attack	---	CS	0.34	52.89	1	0.99	0.11
Gaussian attack	0.001	CS	1.70	45.80	0.96	0.99	0.32
	0.002	CS	2.96	43.41	0.96	0.99	0.47
	0.003	CS	4.81	41.30	0.96	0.99	0.76
	0.01	CS	11.23	37.62	0.96	0.99	2.61
Speckle Noise	0.01	CS	6.03	40.32	1	0.99	0.49
	0.02	CS	9.62	38.29	0.96	0.99	1.02
	0.03	CS	11.09	37.68	0.96	0.99	2.01
	0.1	CS	22.01	34.70	0.96	0.99	3.41
Salt and Pepper Noise	0.01	CS	2.04	45.03	1	0.99	0.30
	0.02	CS	3.44	42.75	1	0.99	0.40
	0.03	CS	13.95	36.68	0.99	0.99	1.15
	0.1	CS	35.90	32.57	0.96	0.99	1.94
Frame cropping		CS	1.57	46.14	0.96	0.99	0.32
Frame swapping		CS	1.22	47.26	1	0.99	0.25
Contrast enhancement		CS	1.53	46.27	1	0.99	0.27
Histogram equalization		CS	161.4	26.05	0.99	0.87	2.51

Fig. 6 shows the PSNR comparison of other watermarking schemes and it indicates that the quality of reconstruction of watermark is better using proposed watermarking technique than other mentioned watermarking schemes while fig. 7 displays comparison of NC values and it indicates that proposed method is more robust than other mentioned existing watermarking techniques. The PSNR calculated by Y. Lui et al. is 40.7357 dB [08] while the PSNR value of 37.63dB in [10], 31.556dB in [11] and 45.35 dB in [13] for transformed domain. The proposed algorithm obtained the PSNR value of 52.89dB and NC=0.99 which found to be better as compare to [8], [10], [11] and [13]. Hence our system is more robust and imperceptible.

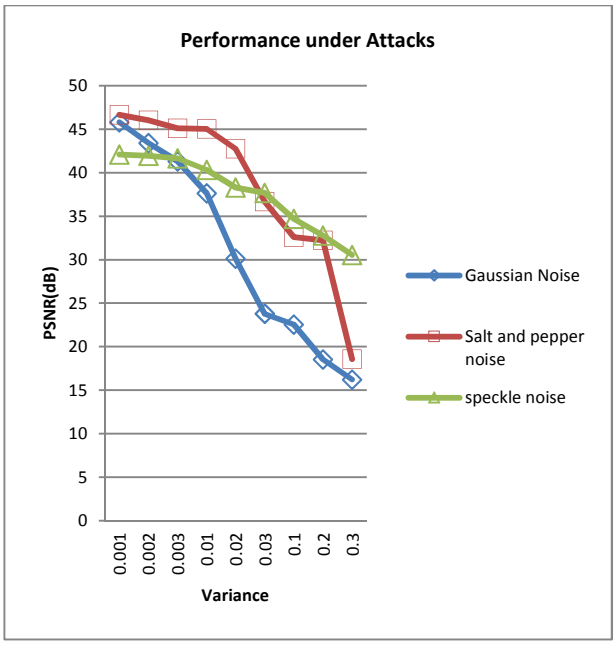

Fig. 5 PSNR comparison between Gaussian attack, Speckle Noise, Salt and Pepper Noise

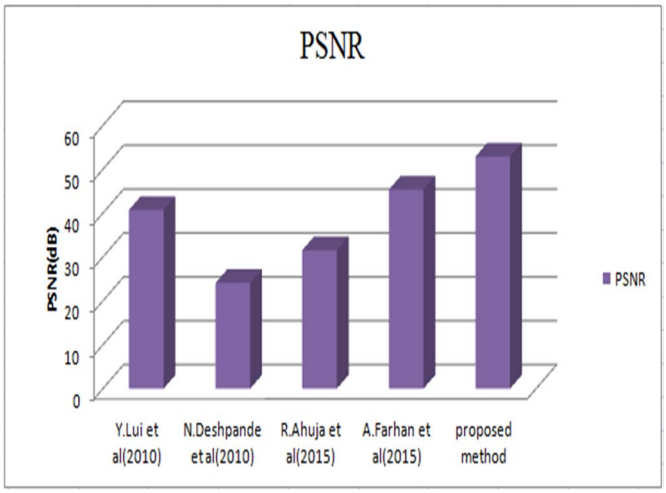

Fig. 6 PSNR comparison of other techniques with proposed method

The proposed technique imparts spatial domain watermarking technique rather than transform domain techniques. Comparing with the transform domain techniques, the proposed method is easy to implement and requires no transformation. From the compared PSNR and NC results, it is observed that the proposed technique shows more robust than DCT based techniques proposed by N. Deshpande et al. [10], DFT based watermarking proposed by Y. Liu et al. [8] and DWT based watermarking algorithm presented by A. Farhan et al. [13].

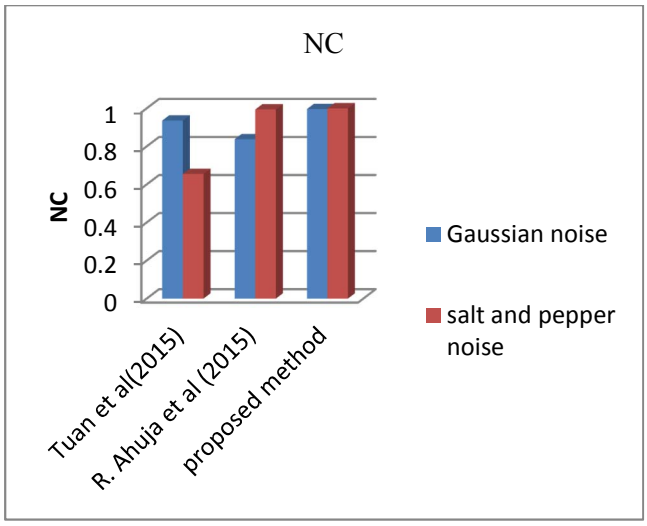

Fig. 7 NC Comparison of existing techniques with proposed method

7. Conclusion

The experimental result shows that proposed algorithm offers better imperceptibility, robustness and security than traditional video watermarking techniques as PSNR value is 52.89 dB, NC is 0.99, SSIM is 0.99 and BER is 0.1. The simulation results also claim that developed spatial domain algorithm shows increase in PSNR value and reduce complexity than any existing techniques. The hardware implementation of the proposed algorithm can be done using FPGA (Field Programmable Gate Array) for real time applications in future.

References

[1] A. Kunhu, Nisi K, S. Sabnam, Majida A and S. AL-Mansoori, "Index mapping based hybrid DWT-DCT watermarking technique for copyright protection of videos files," Online International Conference on Green Engineering and Technologies (IC-GET), Coimbatore, pp. 1-6, 2016.

[2] I. J. Cox, J. Kilian, F. T. Leighton and T. Shamoon, "Secure spread spectrum watermarking for multimedia," IEEE Transactions on Image Processing, vol. 6, no. 12, pp. 1673-1687, Dec 1997.

[3] P. Swati, A. Katharotiya and M. Goyani, "A Survey on Digital Video Watermarking," International Journal of Comp. Tech. Applications, vol. 2, no. 6, pp. 3015-3018, Dec 2011.

[4] S. Kumar, A. Gupta, A. Chandwani, G. Yadav and R. Swarnkar, "RGB image watermarking on video frames using DWT," 5th International Conference, The Next Generation Information Technology Summit (Confluence), Noida, pp. 675-680, 2014.

[5] T. Tabassum and S. M. M. Islam, "A digital video watermarking technique based on identical frame extraction in 3-Level DWT," 15th International Conference on Computer and Information Technology (ICCIT), Chittagong, pp. 101-106, 2012.

[6] N. Dey, P. Das, A. B. Roy, A. Das and S. S. Chaudhuri, "DWT-DCT-SVD based intravascular ultrasound video watermarking," World Congress on Information and Communication Technologies, Trivandrum, pp. 224-229, 2012.

[7] S. M. Sakthivel and R. Sankar, "A real time watermarking of grayscale images without altering it's content," International Conference on VLSI Systems, Architecture, Technology and Applications (VLSI-SATA), Bangalore, pp. 1-6, 2015.

[8] Y. Liu and J. Zhao, "A new video watermarking algorithm based on 1D DFT and Radon transform," Signal Processing, vol. 90, no. 2, pp. 626-639, Aug 2010.

[9] T. T. Nguyen and D. Dinh Nguyen, "A robust blind video watermarking in DCT domain using even-odd quantization technique," International Conference on Advanced Technologies for Communications (ATC), Ho Chi Minh City, pp. 439-444, 2015.

[10] N. Deshpande, A. Rajurkar and R. Manthalkar, "Robust DCT based video watermarking algorithms for assorted watermarks," 2nd International Conference on Signal Processing Systems, Dalian, vol. 6, pp. 320-324, Jul 2010.

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

[12] L. Narkhedamilly, V. P. Evani and S. K. Samayamantula, "Discrete Multiwavelet–Based Video Watermarking Scheme Using SURF," ETRI Journal, vol. 37, no. 3, pp. 595-605, 2015.

[13] Farhan A., F. Kurdahi, A. Eltawil and A. Aljumah, "DWT-based watermarking technique for video authentication," IEEE International Conference on Electronics, Circuits, and Systems (ICECS), Cairo, pp. 41-.44, 2015

[14] K. J. Giri and R. Bashir, "Digital Watermarking: A potential solution for multimedia Authentication", Springer, Intelligent technique in Signal Processing for Multimedia Security, pp. 93-112, 2017.

[15] M. Ghalejughi, M. Ali Akhee, "Video Watermarking in the DT-CWT Domain UsingHyperbolic Function," IEEE 13th International ISC Conference on Information Security and Cryptology, pp. 97-100, 2016.

[16] K. N. Sowmya, H.R. Chennamma, "Video Authentication using Digital Signature- A Study," Springer, 1st International Conference on Computational Intelligence and Informatics, 2017.