Application of Video Watermarking Using Subdivision Technique to Enhance Information Security

Mahesh Gangarde, Janardhan Chitode and Shruti Oza
(Corresponding author: Mahesh Gangarde)
Department of Electronics Engineering, Bharati Vidyapeeth Deemed University College of Engineering
Satara Road, Pune 411043, India
(Email: maheshgangarde@yahoo.co.in, j.chitode@gmail.com)
(Received June 21, 2017; revised and accepted Oct. 21, 2017)

Abstract

This paper proposes an innovative technique of watermark video security using Watermark Sub-Division method. The main objective of this paper is to demonstrate Video Watermark Subdivision Algorithm (VWSA) to secure watermarked secret information. In this algorithm watermarked secret data is subdivided into suitable parts and pixel value of every part is embedded with the same pixel value of a selected frame of video and locates the respective offsets as secret key. At the receiver end the same pixel values are correlated with the Red, Green, Blue (RGB) plane of frames and watermark secret data is recovered based on the amount of correlations achieved. We have applied various types of attacks on watermarked video during transmission and recovered both original video and watermarked secret data without any loss of information. The simulation results demonstrate that the security parameters are improved and the embedded watermark is robust and invisible. Peak Signal to Noise Ratio (PSNR) and Similarity Index (SI) measurable parameters are also calculated to test the quality and matching performance between the original watermark and the extracted watermark to achieve imperceptibility.

Keywords: Attacks; Information Security; Video Watermarking; VWSA

1 Introduction

Nowadays internet plays a very important role in digital multimedia tools like YouTube, Facebook, WhatsApp, Twitter which contain videos for sharing secret information. When such information is sent from the transmitter to the receiver, the major concerns are security of secret watermark data, watermark embedding capacity and good recovery of both original video and watermark secret data. Hence it is always better to provide an information security model to all multimedia [8, 16] tools during transmission. Due to this requirement of digital multimedia, video watermarking can provide a perfect solution for this issue. With today's expanding development of digital multimedia, video watermarking technology plays an important role in copy control, video authentication [3] and copyright protection. Data security is the primary concern when using any media of communication. Our objective is to provide higher data security to protect the watermarked data [1] over the communication channel.

2 Related Work

In 2016, a hybrid algorithm was developed by Kunhu *et al.* which use both DCT and DWT. Index mapping table was used to convert the color watermark logo into the 3 bit index. Then 2-level wavelet decomposition was applied to the selected channel to a particular band which was then divided into 8x8 block and DCT was applied. Then, the location of some coefficients was selected for hiding [8]. Su *et al.* presented a blind watermarking technique which hid the watermark into the blue component of RGB image in the spatial domain. For embedding the watermark, the watermark was divided into four parts and then embedded into different locations of the host image by directly modifying pixel values in the spatial domain [17]. The paper [16] has suggested an effective watermarking technique to secure multimedia data. They explained video watermarking system with image as a watermark using alternative pixels flipped shared under wavelet. In 2008, Do *et al.* gave the concept of digital video watermarking technique using the pixel value histogram watermark which was more robust to camcorder recording attacks and geometric distortions to improve the robustness against geometric synchronization.

To make it imperceptible watermark is adjusted

roughly according to human visual system which shows that proposed technique was more robust to different attacks such as camcorder recording attack and video processing attacks such as MPEG compression. The proposed method was evaluated using different video sequences and it indicates that watermarked video quality is good with average PSNR equal to 45.64dB which is less secure [3]. The paper [2] has suggested the concepts of video watermarking against various attacks using Discrete Wavelet Transform (DWT) technique and Principle Component Analysis (PCA) transform to improve the robustness. The proposed method has applied various attacks on watermarked video to improve the performance against a wide range of attacks with average PSNR equal to 31.65dB and NC equal to 0.8786 which was not correlated to original video, hence it was less secure. Chaluvadi *et al.* has developed an efficient image tamper detection and recovery technique using dual watermarking technique.

The proposed algorithm used two copies of watermark; if one copy is destroyed, watermark is recovered with the other copy of watermark message by embedding more than one bit in 5-MSBs [4, 9]. The result of proposed technique was tested which showed that it is more efficient than Lee and Shingen's method with PSNR 45.85dB [1]. Na Wang *et al.* explained block-based watermarking technique for tamper detection and recovery with color image. In this proposed scheme, RGB channel is divided into blocks and the watermark insertion space is generated by manipulating Least Significant Bit of each targeted block to zero which is used for authentication and recovery codes. Simulation result showed that the proposed technique successfully identified the tampered position and recovered with visual quality with maximum PSNR value of 44.362dB [19]. An efficient video watermarking technique is proposed by Osama based on SVD in DCT domain. In this method video frames are transformed using DWT technique with two resolution levels and error correction code is applied.

In order to increase the robustness, the watermark is embedded with spatial and temporal redundancy [6, 12, 18]. The watermark was tested against different attacks and the proposed watermarking scheme was compared with other schemes [5]. In 2015, Majid *et al.* has presented blind video watermarking technique for verification of ownership using CDMA techniques with binary image as a watermark. In this technique watermark is scattered into different frequency sub-bands of wavelet and during extraction process original video is not required. The proposed technique has good robustness against different video watermarking attacks such as frame dropping, frame averaging and Gaussian noise and evaluated this method with security parameters like PSNR, MSE and SSIM [10]. As video copyright protection is strongly concerned, a robust video watermarking scheme is necessary. In order to design a robust [7], invisible, blind andnon-removable video watermarking scheme, a survey and investigation has been done on multimedia security issues and multimedia watermarking scheme.

Various watermarking scheme are compared and evaluated. Based on these, a new approach and procedures for multimedia security based on watermarking are proposed. At the same time, Sowmya [15] error correcting code is extracted from the video channel and embedded into the audio channel, which provide extra information for recovery of extracted watermark. Shojanazeri and Wan present the state of the art in video watermarking techniques. It provides a critical review on various available techniques. In addition, it addresses the main key performance indicators which include robustness, speed, capacity, fidelity, imperceptibility and computational complexity. The advancement of Internet services and various storage technologies, made video piracy as an increasing problem particularly with the proliferation of media sharing through the internet. This method performed better in JPEG compression of 80% as the PSNR equaled to 37.715dB and the NC for the extracted watermark from LL is 0.983 despite of HH sub band which is 0.162.The PSNR after resize is 41.207dB [13].

2.1 Main Contribution

The main contribution of this paper is to improve concealed watermark secret data security, perceptibility and its robustness. As video is made up of number of still images/frames, we have selected any frame to conceal secret watermark image using VWSA technique. During transmission of watermarked video we have applied five different types of attack on watermarked video and obtained important key security parameters before concealing, after concealing and after recovering from watermarked video. The values of key security parameter like PSNR, NC, MSE, SI and Histogram were not changed and we recovered secret watermark image without any loss of information. Thus it improves security, perceptibility and robustness of proposed security model for video watermarking using VWSA.The rest of the paper is organized as follows. Section 3 indicates proposed video watermarking using VWSA, Section 4 shows key security parameters and its importance and Section 5 gives different attacks on watermarked video, Section 6 indicates simulation results & discussion and in the last section conclusion and references are presented respectively.

3 Proposed Security Model of Video Watermarking

The input to proposed security model is any type of video. The input video is split into number of frames and audio. Before concealing watermark secret data we have divided it into number of small parts and every small part is concealed using VWS algorithm. In this paper, all embedding procedures are explained for single block of watermark secret image. We have obtained major security parameter like PSNR, MSE, NC and histogram of secret watermark

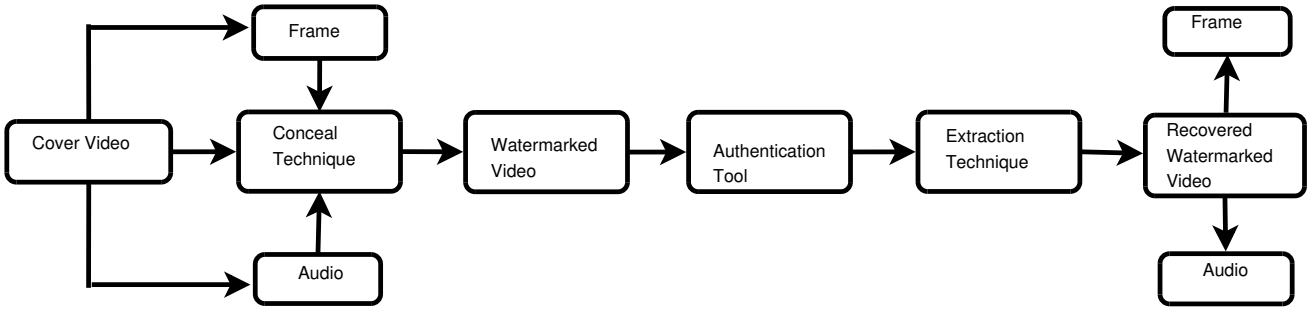

Figure 1: Block diagram of proposed video watermarking security model

data before embedding. Once concealing process has been done, watermarked video is obtained which is sent from transmitter to receiver. Authentication tool is used to cross check the incoming watermarked video in terms of PSNR, MSE, NC and histogram. If these major security parameters are matched with original watermark secret data, then it is sent to the receiver end, otherwise authentication tool stops the incoming watermarked video. We have used secret key which is known to both the parties. After matching the security parameters, authentication tool allows sending authenticate watermark video to receiver with watermark extraction process as shown in Figure 1.

3.1 VWSA for Video Watermarking

To improve the watermarked concealed capacity and security, we have divided secret watermark data into number of blocks and each block is embedded by using key structure. As video contains large number of frames,hence large numbers of locations are available to embed the secret data and hence embedding capacity is increased. When such watermarked video is sent from transmitter to receiver it is very difficult to understand in which frame of video secret watermark data is embedded, hence security of proposed technique is improved. In watermark subdivision technique, pixel values are located on the basis of matching between watermark pixel values and frame pixel values which forms secret key as shown in Figure 2. We have obtained the pixel values from watermark secret image and located those pixel values into selected frames of video to improve the embedding capacity and enhance the security of secret watermark information. The Figure 2 shows the working model of proposed video watermarking algorithm using VWSA technique which improves the conceal capacity and security of secret data. We have considered the color image as watermark data, converted it into its pixel values and found out those pixel values in cover video frame. An example shown in Figure 2, pixel value 5, 0 and 89 matched with frame pixel values by different locations. Record frame number and the locations of matched pixel values between secret watermark image with cover video frame in secret key structure shown in Matrix (d) which is used for higher data security or privacy. Continue this process till the matching of pixel values of watermark image with cover video frames.

3.2 Embedding Procedure with Example

The Algorithm 1 is explained with an example of first frame of cover video of size 8x8 as shown in Matrix (a) and watermark image of size 4x4 as displayed in Matrix (b). Let $w(i,j)$ and $f(i,j)$ be the pixel location in watermark and cover frame respectively. The pixel value at $w(1,1)$ is 251, will be searched row-wise in the selected frame of video. This value is found to be matched at $f(1,3)$ i.e. shown in bold in Matrix (c). So note that frame number and location of $f(1,3)$ in key structure displayed in Matrix (d) which occupies three locations of key structure. First two locations of key structure indicate the size of watermark secret image and the third location indicates the frame. Similarly the next pixel value of watermarked image $w(1,2)$ i.e. 250 will be searched in Matrix (a) and the match is found at $f(4,8)$ then stored respective frame number and pixel location in key structure. If watermarked pixel value is not found in first frame the search it in the next frame and continue. When match is found, the respective frame number and the location of that pixel stored in key structure and so on. Steps 6, 7, and 8 are explained respectively in detail as follows:

If $(f(i,j) == w(i,j))$ Note the frame number and pixel location in key structure elseif $(f(i,j) == (w(i,j)+1))$ Note the frame number and pixel location in key structure elseif$(f(i,j) == (w(i,j) \vee 1))$ Note the frame number and pixel location in key structure.

4 Key Security Parameters and Its Importance

4.1 Similarity Index (SI)

Similarity Index is used to find similarity between two images, the measurement of image quality is based on an initial uncompressed or distortion free image as reference [10]. In the proposed security model, we have obtained SI with respect to original video which is found to be similar to each other hence our proposed method is

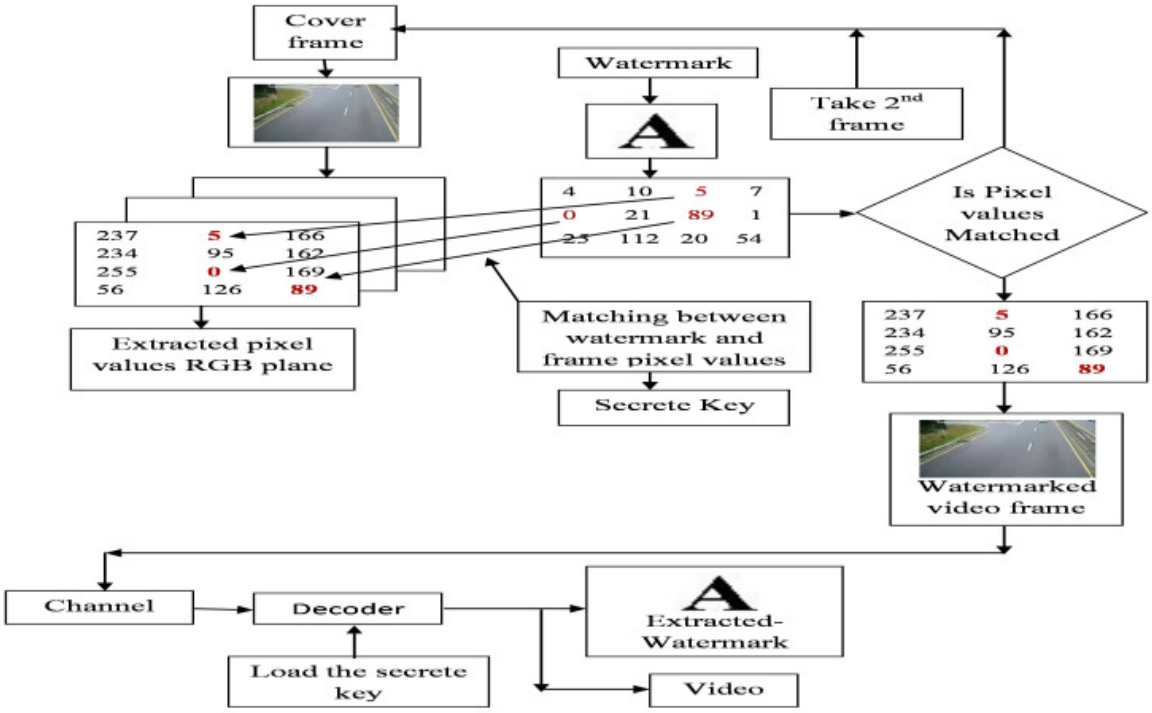

Figure 2: Process of embedding and extracting secret watermark image using VWS algorithm

255	224	251	235	234	245	250	251
168	225	209	215	249	202	238	122
123	231	206	253	251	199	219	215
111	244	236	255	240	200	237	250
125	249	245	250	251	123	231	206
229	251	202	238	122	126	244	236
217	240	199	219	215	125	249	202
246	248	200	237	250	236	252	254

Matrix (a). Pixel matrix of cover frame

251	250	209	215
123	244	201	215
228	255	251	189
112	236	238	250

Matrix (b). Pixel matrix of Watermark image

255	224	251	235	234	245	250	251
168	225	209	215	249	202	238	122
123	231	206	253	251	199	219	215
111	244	236	255	240	200	237	250
125	249	245	250	251	123	231	206
229	252	202	238	125	126	244	236
217	240	190	219	215	125	249	202
246	248	200	237	250	236	252	254

Matrix (c). Pixel matrix of Watermarked Frame

4	4	1	1	3	1	4	8	-	-	-

Matrix (d). Key Structure of size (3Q+2)

Figure 3: Pixel matrix and key structure

Algorithm 1 Algorithmic Steps

1: Begin
2: Obtain the cover video in RGB format.
3: Take color image as watermark data (32x32, 64x64, 128x128and 256x256).
4: Convert the secret image to gray scale image.
5: Search first pixel value of the gray scale image into first frame of video for matching the pixel values.
6: If it is not matched in the first cover frame then search in the next frame andcontinue this up to last frame.
7: When match is found then that frame number of video and location of pixel is stored in structure key.
8: If match is not found in all frames then watermarked pixel value is incremented by 1 i.e. w(i,j)=w(i,j)+1, then new pixel value i.e. w(i,j) is searched in all frames of the video starting from the first frame.
9: If again match is not found decrement watermark pixel value by 1 i.e. w(i,j)=w(i,j)-1, then again search in all frames.
10: Repeat steps vii and viii upto match condition, and after that perform step vi for storing the location of pixel in structure key.
11: Convert all matching pixel locations separately for R, G and B planes.
12: Repeat all above steps for all pixel values of watermarked image.
13: Generate the watermarked video with above watermark subdivision algorithm.
14: Reconstruct the watermark image by using respective locations from secret key structure.
15: End

more secure as shown in Equation (1):

$$SI = \frac{(2\eta_x\eta_y + a_1)(2\kappa_{xy} + a_2)}{(\eta_x^2 + \eta_y^2 + a_1)(\kappa_x^2 + \kappa_y^2 + a_2)} \quad (1)$$

Where η_x and η_y are the average of x and y respectively, K_{xy} is covariance of x & y, a_1 and a_2 are two variables to stabilize the division with weak denominator.

4.2 Peak Signal to Noise Ratio (PSNR)

PSNR is most commonly used to measure the quality of reconstruction of original secret data. Its typical range is 35dB to 70dB. A higher PSNR generally indicates that the reconstruction is of higher quality, which can be calculated using Equation (2):

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

Where MAX is the maximum pixel value of the image, MSE [10] is the sum over all squared value differences divided by image size, determined by Equation (3):

$$MSE = \frac{1}{MN}\sum_{mn}(P(m,n) - Q(m,n))^2 \quad (3)$$

Where $P(m,n)$ and $Q(m,n)$ represents two images and M and N represents total number of pixels of secret frame of video and secret watermark image.

4.3 Normalised Correlation (NC)

Normalised Correlation shows the similarities between original image and secret image extracted from watermarked video.We have calculated the NC of selected frame of original video before embedding secret data and after embedding secret data which are exactly identical to each other as shown in Equation (4):

$$NC = \frac{1}{n}\sum_{xy}\frac{(f(x,y) - \overline{f})(t(x,y) - \overline{t})}{m_f m_t} \quad (4)$$

Where n is the number of pixels in *t(x,y)* and *f(x,y)*, $\bar{f}$ is the average of f and m_f is standard deviation of f. It measure immunity of watermark against attacks to remove or degrade it. Maximum Normalised Correlation indicates better Robustness [5].

5 Different Attacks on Watermarked Video

5.1 Histogram Equalization

It is used to remove the embedded data from watermarked video.The basic concept of histogram equalization is to enhance contrast of watermark histogram. Histogram equalization is an example of image enhancement technique [19]. To apply the histogram equalization attack we have modified the values of watermark image to stretch the histogram and controlled the desired number of grey scale value from the watermark image pixel value as shown in Figure 4.

5.2 Gaussian Noise Attack

In the proposed technique we have applied Gaussian noise [10] to original video and watermarked video. After Gaussian attacks our original and watermark video does not change, hence the proposed method is more robust against this attack as indicated in Figure 5.

5.3 Salt and Pepper Attack

Impulsive noise is also sometimes called as salt and pepper attack or spike attack. For selected frame of watermark videowe have obtained dark pixel in bright region and bright pixel in dark region. It is the process of removing the watermark image from watermarked video without attempting to break the security of the algorithm [3, 8]. It is a noise attack in which salt is considered as non-zero value 255 (salt) and pepper as 0 (pepper) as given in Figure 6.

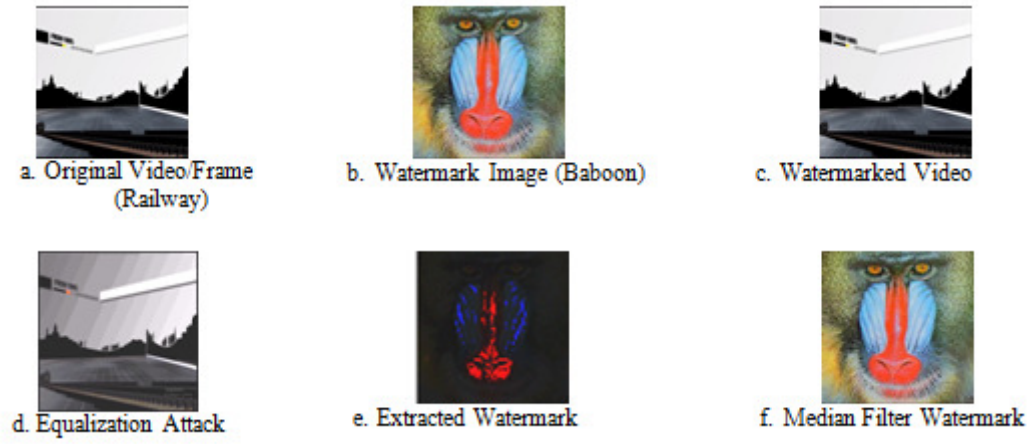

Figure 4: Historgram equalization

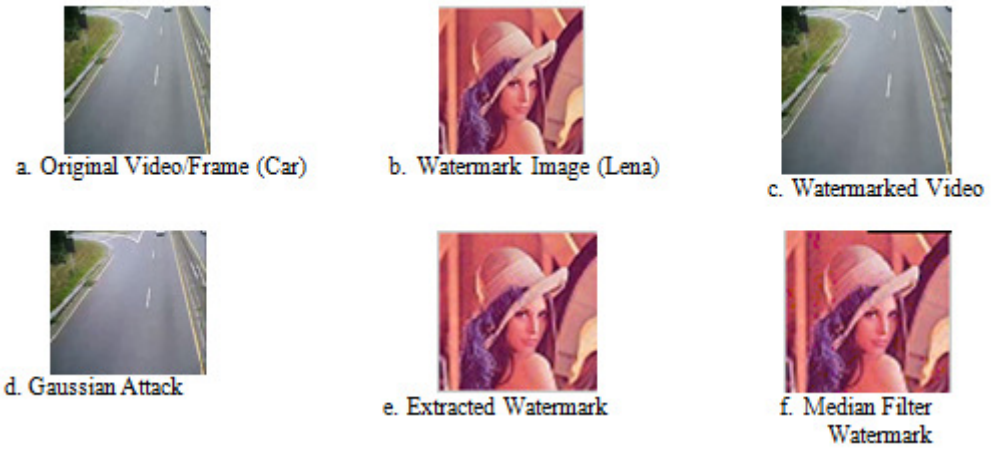

Figure 5: Gaussian attack

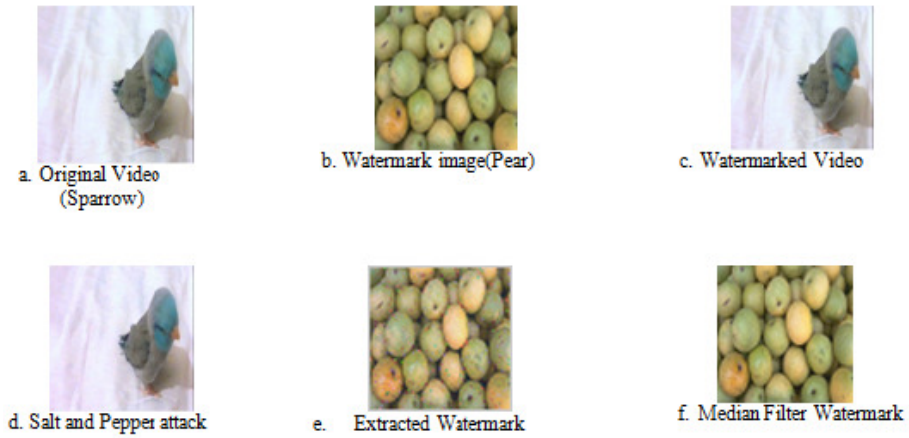

Figure 6: Salt and pepper attack

5.4 Contrast Enhancement Attack

Contrast enhancements improve the perceptibility of embedded data by enhancing the brightness difference between embedded data and their backgrounds. We have applied contrast enhancement attack [3] on selected frame of both original and watermarked video which looks identical as shown in Figure 7.

5.5 Speckle Noise Attack

Speckle attack is noise attack which is applied to test the robustness of the system [2, 14]. It is added to the watermarked video and calculated the PSNR between the original and watermarked video and in between the extracted and original watermark secret message to identify the effect of attack on the watermark after attacking process as shown in Figure 8.

6 Simulation Results and Discussion

We have simulated results through number of videos of different video formats like .Avi, .Flv, .Wmv and .Mp4 and watermark images like Lena, Baboon, Pepper and Pears of different sizes. Table 1 indicates frame wise analysis of SI for different video format. For .Avi video of frames 220 we have used Lena as secret data of size 64x64. For .Avi car video of frames 220, we have embedded Lena watermark image of size 64x64 with and without attack. The value of PSNR is 49.97dB without attacks while with attacks average PSNR is 25.06dB. We have applied median filter so noise in the pixel has been removed and we have obtained PSNR = 49.67dB. As we have embedded baboon image of same size (64x64) with attack and without attack, the PSNR value is 49.67dB without attack while 37.79dB with attack as shown in 9. We have applied median filter with all types of attack and last column shows the values with Gaussian attack. Table 2 gives the functionality comparison between Taun's method [11], Osama [5], Ranjeet [14] and our proposed video watermarking security model in terms of PSNR, SI, NC, attacks, robustness and perceptibility. As we have divided the secret watermark image into four equal parts and embedded it into selected frames of video, hence it is very difficult to understand in which frame, the secret data is hidden so security of watermark video is increased. We have observed five different attacks on watermark video during transmission and calculated PSNR, SI, NC, MSE and Histogram after recovering from watermark video which is identical to each other hence perceptibility of proposed algorithm has increased. We have observed results through .Avi, .Flv and .Mp4 video format having different frame size. We have embedded secret data as images into randomly selected frames of video to generate watermarked video. Median filter is used to remove the unwanted noise which is added during transmission. Hence we have applied median filter after applying different types of attacks. Hence we have recovered our secret data without any loss of information as indicated in Figure 9. Figure 5 indicates the effect of Gaussian attacks. The original .Avi car video of frames 220 of size 410Kb displays in Figure 5(a). Figure 5(b) is the watermark original secret Lena image of size 64x64 before embedding into video. Figure 5(c) is the watermarked video which is exactly identical to original Car video hence perceptibility of proposed system is increased. Figure 5(d) indicates the effects of Gaussian attacks on watermarked video and Figure 5(e) shows extracted secret Lena image with some distortion hence we cannot recover watermark secret data. In the proposed technique we have used median filter to remove the noise from the watermarked video as shown in Figure 5(f).

Figure 4 shows the effect of Histogram Equalization attacks. The original .Avi Railway video of frames 311 of size 746Kb is displayed in Figure 4(a). Figure 4 (b) is the watermark original secret Baboon image of size 64x64 before embedding into video. Figure 4(c) is the watermarked video which use exactly identical to original Railway video hence perceptibility of proposed system is increased. Figure 4(d) indicates the effects of Histogram Equalization attacks on watermarked video and Figure 4(e) shows extracted secret Baboon image with some distortion hence we cannot recover watermark secret data. In the proposed technique we have used median filter to remove the noise from the watermarked video as shown in Figure 4(f).

Figure 7 indicates the effect of Contrast Enhancement attacks. The original .Flv Dog video of frames 335 displayed in Figure 7(a). Figure 7(b) is the watermark original secret Tree image of size 128x128 before embedding into video. Figure 7(c) is the watermarked video which looks exactly identical to original Dog video before attack hence robustness of proposed system is increased. Figure 7(d) indicates the effects of Contrast Enhancement attacks on watermarked video and Figure 7(e) shows extracted secret Tree image with some distortion hence we cannot recover watermark secret data. In the proposed technique we have used median filter to remove the noise from the watermarked video as shown in Figure 7(f). Figure 8 indicates the effect of Speckle Noise attacks. The original .Flv Cat video of frames 410 is displayed in Figure 8(a). Figure 8(b) is the watermark original secret Pepper image of size 128x128 before embedding into video. Figure 8(c) is the watermarked video which are exactly identical to original Cat video hence the security of proposed system is increased. Figure 8(d) indicates the effects of Mean Noise attacks on watermarked video and Figure 8(e) shows extracted secret Pepper image with some distortion hence we cannot recover watermark secret data. In the proposed technique we have used median filter to remove the noise from the watermarked video as shown in Figure 8(f). Figure 6 indicates the effect of Salt and Pepper attacks. The original .Mp4 Sparrow video of frames 390 displays in Figure 6(a). Figure 6(b) is the watermark original secret Pear image of size 256x256 before

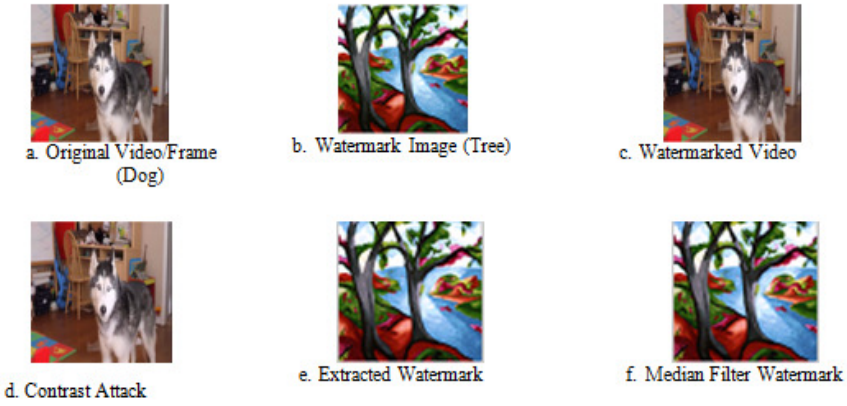

Figure 7: Contrast enhancement

Figure 8: Speckle noise attack

Video	Watermark Image	Size	Parameters	Without Attack	With Attack					
					Gaussian	Salt & Pepper	Histogram	Contrast Enhancement	Speckle Noise	Median Filter
CAR		64x64	PSNR(dB)	49.97	34.36	28.34	15.60	40.67	31.38	49.64
			NC	0.99	0.99	0.99	0.99	0.99	0.99	0.99
			SI	0.98	0.85	0.79	0.76	0.98	0.93	0.98
RAIL WAY		64x64	PSNR(dB)	49.21	34.58	27.05	11.26	42.13	28.74	49.15
			NC	0.98	0.90	0.93	0.90	0.97	0.90	0.98
			SI	0.98	0.76	0.66	0.61	0.98	0.92	0.99
DOG		128x128	PSNR(dB)	50.51	33.40	27.72	18.58	38.84	32.10	49.77
			NC	0.99	0.99	0.99	0.99	0.99	1	0.99
			SI	0.96	0.84	0.71	0.81	0.96	0.94	0.97
CAT		128x128	PSNR(dB)	49.00	33.73	27.24	20.47	39.68	32.51	48.61
			NC	0.97	0.95	0.96	0.95	0.97	0.97	0.97
			SI	0.96	0.83	0.70	0.74	0.95	0.94	0.96
SPAR ROW		256x256	PSNR(dB)	50.62	34.49	27.30	10.79	40.11	28.56	49.95
			NC	1	1	1	0.99	1	1	0.99
			SI	0.97	0.83	0.69	0.57	0.96	0.96	0.98

Figure 9: Security parameters value with five different attacks and without attacks

embedding into video.we have recovered watermark video without any loss of secret information as shown in Figure 6(c). Figure 6(d) indicates the effects of Salt and Pepper attacks on watermarked video and Figure 6(e) shows extracted secret Pear image with some distortion hence we cannot recover watermark secret data. In the proposed technique we have used median filter to remove the noise from the watermarked video as shown in Figure 6(f).

The frame wise analysis is displayed in table 1 for frame numbers such as 21, 41, 61, 81, 101 and 141. Proposed method has been checked by applying five different attacks on watermark video during transmission with NC = 1 and SI = 0.987 which shows that proposed method is more robust than existing methods.

Table 1: Frame wise analysis SI for different video

Frames	Car	Railway	Dog	Cat	Sparrow
21	0.987	0.990	0.972	0.974	0.999
41	0.872	0.762	0.853	0.830	0.837
61	0.721	0.973	0.726	0.708	0.692
81	0.772	0.622	0.822	0.744	0.587
101	0.984	0.987	0.966	0.961	0.971
141	0.932	0.933	0.922	0.927	0.929

Figure 10 shows the histogram of original watermark image (Lena), histogram after embedding watermark (watermarked video) and histogram of extracted watermark. Figure 10(a) indicates Lena as watermark image and figure 10(b) shows its histogram. Watermarked video is indicated in figure 10(c) and figure 10(d) shows its histogram. Figure 10 (e) and figure 10(f)shows the recovered watermark and its histogram respectively. Hence our proposed watermarking system is more imperceptible to any existing techniques.

It is found that the proposed security approach is better than existing video watermarking techniques. Taun's method [11] used the DCT based watermarking using even-odd quantization method where the performance parameters were calculated for different video sequences and watermark under different attacks. The average value of PSNR and SI is 44.44dB and 0.8969 respectively; hence it recovers the secret data with some loss of information. Osama's method [5] applied effects of different attacks like scaling, cropping and rotation on video during transmission which is less secured. As the value of SI is 0.8969 the quality of recovered secret data has some distortion. In the suggested approach we have embedded watermark data as text and image into selected frames of video using video watermark subdivision technique, key security parameters PSNR, SI, NC, MSE are better than those are in Taun's [11], Osama's [5] and Ranjeet's [14] approach.

In SVD based DWT watermarking proposed by Osama, PSNR is compared for different DWT schemes [5]. The PSNR is calculated as 44.82dB and the performance is checked under 4 different attacks. Watermarking in spatial domain is projected by Ranjeet which uses LSB watermarking [14]. The PSNR is calculated for different RGB components of an image separately and the effect of three different attacks is evaluated. The PSNR is about 38.69 and the value of NC is 0.5206. The proposed method shows the average value of PSNR as 46.06dB, SI as 0.9870, and NC as 1 and MSE as 0.0858. The performance parameters are calculated for five different attacks. This shows that the proposed method is more robust than other three different methods. Taun and Osama applied four different attacks while Ranjeet applied only three. As the value of PSNR, SI, NC, MSE are found to be exactly same, the perceptibility, security of hidden data and robustness of proposed system is increased.The Figure 11 shows the average PSNR comparison of other schemes with proposed schemes. The DWT based SVD watermarking scheme proposed by Osama displays the value of PSNR as 44.82dB. Ranjeet's method gives the PSNR of 38.75 dB while 44.71dB is for the DCT based method explained by Tuan. In proposed method the PSNR is 49.89 dB.

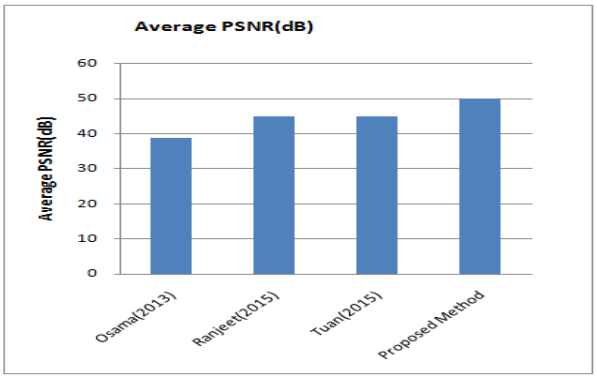

Figure 11: PSNR comparison of other schemes with proposed schemes

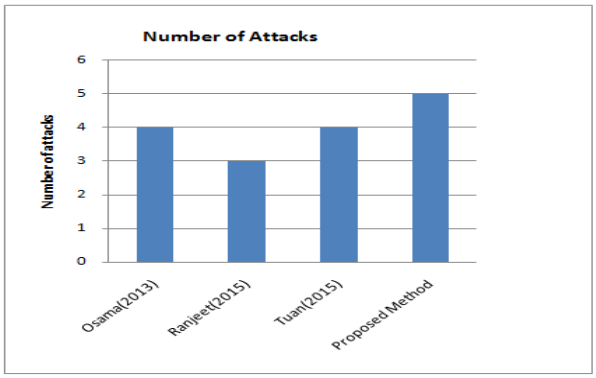

Figure 12: Robustness of other schemes and proposed scheme

Figure 11 shows that our proposed scheme offers better PSNR than other similar schemes. This indicates the quality of reconstruction of watermark is better in proposed method than other mentioned schemes; while Figure 12 shows the number of attacks performed by different techniques.

Method Proposed by Osama survives four different at-

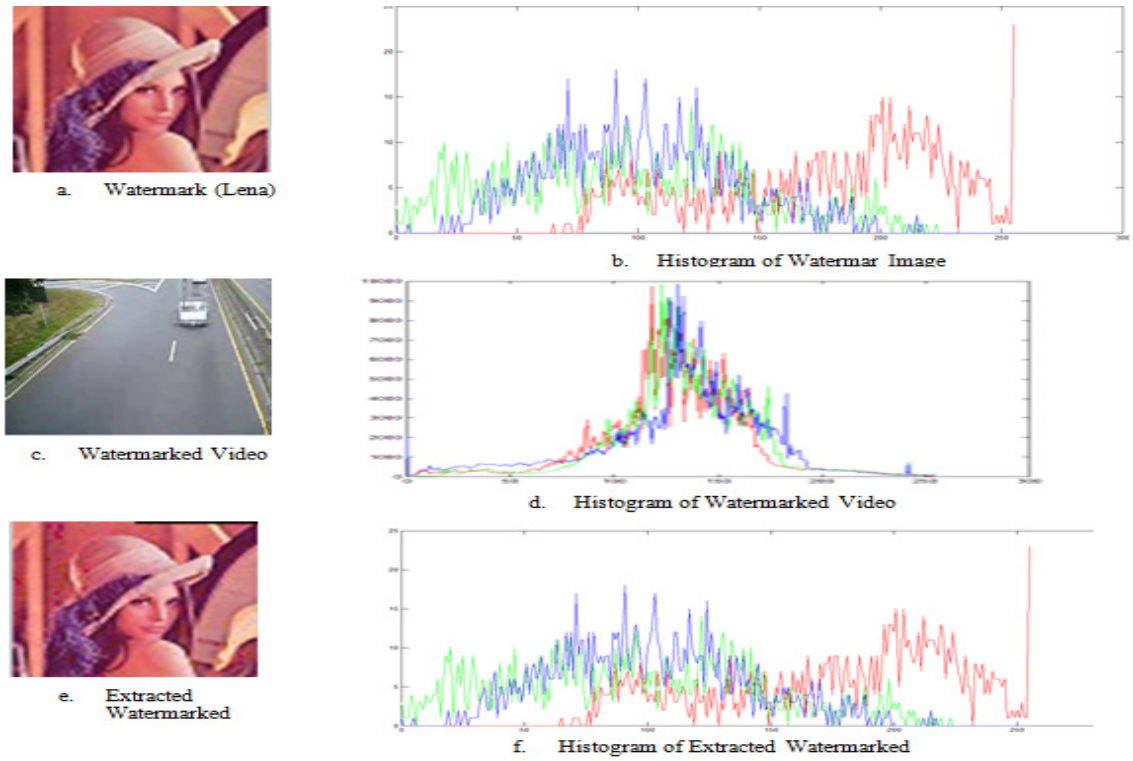

Figure 10: Histogram of watermark image, watermarked video and watermark (secret data) after extraction

tacks while three attacks are applied in Ranjeet's scheme based on LSB technique. Analysis of four different attacks is done by Tuan while the proposed method analyses five different attacks. It indicates that our proposed scheme has more robustness than other scheme.

7 Conclusions

We have presented innovative video watermarking technique to improve security of watermark embedding data with video watermark subdivision algorithm (VWSA). The video watermark technique is tested and verified using standard videos and sample watermark images. The key security parameters PSNR, MSE, NC, SI are calculated before embedding, after embedding and after recovering embedding data from watermarked video. We have applied five attacks on watermarked video during transmission and it is found that the proposed technique is more robust and imperceptible to these attacks. We have compared our result to existing techniques and it is better than existing techniques. In future it can be applied on more video formats with different embedding techniques.

References

[1] S. B. Chaluvadi and M. V. Prasad, "Efficient image tamper detection and recovery technique using dual watermark," in *World Congress on Nature & Biologically Inspired Computing (NaBIC'09)*, pp. 993–998, 2009.

[2] M. A. Chimanna and S. Khot, "Robustness of video watermarking against various attacks using wavelet transform techniques and principle component analysis," in *International Conference on Information Communication and Embedded Systems (ICICES'13)*, pp. 613–618, 2013.

[3] H. Do, C. D, C. H, and K. T, "Digital video watermarking based on histogram and temporal modulation and robust to camcorder recording," in *IEEE International Symposium on Signal Processing and Information Technology*, pp. 330–335, 2008.

[4] D. Essaidani, H. Seddik, and E. B. Braiek, "Asynchronous invariant digital image watermarking in radon field for resistant encrypted watermark," *International Journal of Network Security*, vol. 18, no. 1, pp. 19-32, 2016.

[5] O. S. Faragallah, "Efficient video watermarking based on singular value decomposition in the discrete wavelet transform domain," *AEU-International Journal of Electronics and Communications*, vol. 67, no. 3, pp. 189–196, 2013.

[6] M. S. Hwang, C. C. Chang, K. F. Hwang, "Digital watermarking of images using neural networks", *Journal of Electronic Imaging*, vol. 9, no. 4, pp. 548–556, Jan. 2000.

[7] D. Jiang, J. Kim, *et al.*, "A spread spectrum zero video watermarking scheme based on dual transform domains and log-polar transformation," *Inter-*

Table 2: Comparison of proposed technique with existing watermarking methods

Parameters	Taun (2015)[11]	Osama (2013)[5]	Ranjeet (2015)[14]	Proposed method
PSNR	44.89	44.83	38.70	50.51
	44.72	44.82	38.69	49.97
	44.53	44.82	38.86	49.21
SI	0.8969	-	-	0.98
NC	-	-	0.5206	1
MSE	-	-	-	0.08
No. of attacks applied	04	04	03	05
Watermarking	Video	Video	Image	Video
Robustness	-	-	Yes	Yes
Perceptibility	-	-	-	Yes

national Journal of Multimedia and Ubiquitous Engineering, vol. 10, no. 4, pp. 367–378, 2015.

[8] A. Kunhu, K. Nisi, S. Sabnam, A. Majida, and A.-M. Saeed, "Index mapping based hybrid dwt-dct watermarking technique for copyright protection of videos files," in *International Conference on Green Engineering and Technologies (IC-GET'16)*, pp. 1–6, 2016.

[9] L. Laouamer, O. Tayan, "An efficient and robust hybrid watermarking scheme for text-images," *International Journal of Network Security*, vol. 18, no. 6, pp. 1152-1158, 2016.

[10] M. Masoumi, M. Rezaei, and A. B. Hamza, "A blind spatio-temporal data hiding for video ownership verification in frequency domain," *AEU-International Journal of Electronics and Communications*, vol. 69, no. 12, pp. 1868–1879, 2015.

[11] T. T. Nguyen, D. D. Nguyen, "A robust blind video watermarking in DCT domain using even-odd quantization technique," in *International Conference on Advanced Technologies for Communications (ATC'15)*, pp. 439–444, 2015.

[12] J. Qin, R. Sun, X. Xiang, H. Li, H. Huang, "Anti-fake digital watermarking algorithm based on QR codes and DWT," *International Journal of Network Security*, vol. 18, no. 6, pp. 1102-1108, 2016.

[13] H. Shojanazeri, W. A. W. Adnan, and S. M. S. Ahmad, "Video watermarking techniques for copyright protection and content authentication," *International Journal of Computer Information Systems and Industrial Management Applications*, vol. 5, pp. 652–660, 2013.

[14] R. K. Singh, D. K. Shaw, and M. J. Alam, "Experimental studies of LSB watermarking with different noise," *Procedia Computer Science*, vol. 54, pp. 612–620, 2015.

[15] K. N. Sowmya and H. R. Chennamma, *Video Authentication Using Watermark and Digital Signature - A Study*, pp. 53–64, Springer Singapore, 2017.

[16] B. Sridhar and C. Arun, "An enhanced approach in video watermarking with multiple watermarks using wavelet," *Journal of Communications Technology & Electronics*, vol. 61, no. 2, pp. 165, 2016.

[17] Q. Su and B. Chen, "Robust color image watermarking technique in the spatial domain," *Soft Computing*, Jan. 2017. (https://doi.org/10.1007/s00500-017-2489-7)

[18] D. Vaishnavi, T. S. Subashini, "A secure and robust image watermarking system using normalization and Arnold scrambling," *International Journal of Network Security*, vol. 18, no. 5, pp. 832-841, 2016.

[19] N. Wang, C. H. Kim, "Color image of tamper detection and recovery using block based watermarking," in *IEEE 4th International Conference on Embedded and Multimedia Computing (EM-COM'09)*, 2009.

Biography

Mahesh Gangarde is pursuing Ph.D.(Electronics Engineering) from Bharati Vidyapeeth University College of Engineering, Pune. He has received B.E. from Shri Tuljabhavani College of Engineering, Tuljapur in 2002 and M.E. from Bharati Vidyapeeth University College of Engineering, Pune in 2009. His research area is image/video processing and security.

J. S. Chitode is a professor received the B.E. degree in Industrial Electronics Engineering from Bharati Vidyapeeth University, Pune, Maharashtra in 1991. He received M.E. degree from College of Engineering(COEP),Pune at University of Pune from Maharashtra, India in 1995. He has received Ph.D. degree in Electronics from Bharati Vidyapeeth Deemed University, India in 2009. Currently he is a professor in the Bharati Vidyapeeth Deemed University College of Engineering, Pune (India). His research interest includes Signal processing, Speech Synthesis, Digital Communication, etc. He is actively participating as a member of different professional research societies, like IEEE, ISTE, etc