A Novel SecureVideo Watermarking Scheme using DWT &Random Frame Selection

Pavneet K Athwal
Department of Computer Science Engineering
RIMT, M.G.G, Punjab,India

Ranpreet Kaur
Department of Computer Science Engineering
RIMT, M.G.G, Punjab,India

Anuj K Gupta
HOD, Department of Computer Science Engineering
RIMT,M.G.G, Punjab, India

Abstract - Digital videowatermarking is the enabling technology to prove ownership of copyrighted material, to solve the problem of piracy and to detect the originator of illegally made copies.In this paper, to solve the authentication problem an effective, imperceptible and secure blind video watermarking algorithm is proposed which uses an encryption key to select the random frames of video in which watermark information is embedded uniformly throughout the video. To keep the algorithm imperceptible DWT technique is used for embedding.The performance of algorithm is tested using MATLAB software on video of "traffic" and watermark image of 256 X 256.The experimental results show that the proposed scheme is highly imperceptible, less time consuming, more secure and highly robust against various attacks.

General Terms - Video Watermarking, Security, Imperceptibility, Robustness

Keywords - Video Watermarking, PSNR,MSE, BER

I. INTRODUCTION

In the past duplicating art work was quite complicated and required a high level of expertise for the counterfeit to look like the original. However, in the digital world this is not true. Now it is possible for almost anyone to duplicate or manipulate digital data and not lose data quality. So watermarking has become a major field to solve the problems of illegal manipulation, distribution and piracy of digital videos [1, 2].Video watermarking is the process of embedding copyright information or verification messages in video bit streams.Video watermarking research received less attention than image watermarking due to its inherit difficulty, however, many algorithms have already been proposed [3,4,5,6].

The information which is embedded is called watermark. It can be text or an image.Two types of digital watermarks may be distinguished, depending upon whether the watermark appears visible or invisible to the casual viewer.Visible watermarks can be a logo or text on frames of videos either in all frames or in just a few selected frames. If it is present in selected frames then it passes off without being noticed, due to high frame rate. Invisible watermarks or Hidden watermarks on other hand are present in the file in such a way that they cannot be sighted but have to be extracted.

Watermarking algorithm should be imperceptible i.e embedding should not affect the quality of video. It should also be robust to various signal processing operations i.e. watermark could not be destroyed or degraded after any type of video manipulations.

Watermarking algorithm can be blind or non blind. If the extraction process needed the original data for the recovery of watermark from watermarked video then it is said to be non blind scheme of watermarking. If watermark can be recovered from only watermarked video without any need of original data then it is called blind scheme of watermarking.

This scheme applied to videos shows that it consumes very small time to embed the watermark information and it is highly imperceptible, exhibits high robustness againstvarious attacks& more secure scheme due to use of secret key and random frame selection.

II. PROBLEM STATEMENT

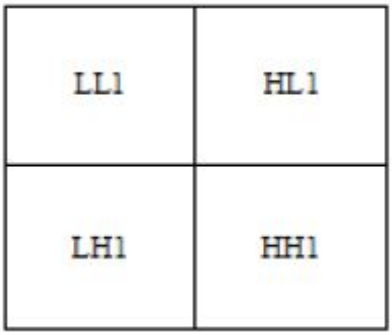
As digital video-based application technologies grow, such as Internet video, wireless video,Videophones, and video conferencing, the problem of illegal manipulation, copying, distribution and piracy of digitalvideo rises more and more. The problem of this paper research work is to solve the authentication problem and embed the watermark in such a way that it could not be removed or degraded from the video using the proposed algorithm of random frame selection through secret key.

III. THEORETICAL BACKGROUND

The proposed work requires certain theoretical considerations related to the concept of Entropy &its performance parameters. The following sections contain a brief description of these concepts.

3.1 Discrete Wavelet Transform (DWT)

Wavelet transform is a multi-resolution decomposition of a signal. The low pass filter applied along a certain direction extracts the low frequency (approximation) coefficients of a signal. On the other hand, the high pass filter extracts the high frequency (detail) coefficients of a signal. In 2D applications, for each level of decomposition, first perform the DWT in the vertical direction, followed by the DWT in the horizontal direction. After the first level of decomposition, there are 4 sub-bands: LL1, LH1, HL1, and HH1.



3.2 Performance measures

Imperceptibility, robustness, security, complexity &data payload are considered as performance parameters for the proposed watermarking Algorithm.

3.2.1 Imperceptibility

Imperceptibility means that the perceived quality of the video should not be distorted by the presence of the watermark.As a measure of the quality of a watermarked video, Bit Error Rate (BER), Peak Signal toNoise Ratio (PSNR),and Mean Squared Error (MSE) is calculated between the original video frame and the corresponding watermarked frame [8].

3.2.1.1 Mean squared error (MSE)

To measure the similarity between the original video frame and watermarked frame an error signal is computed by subtracting the watermarkedframe from the original frame,and then computing the average energy of the error signal. The MSE is given by equation

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(x(i,j) - y(i,j))^2 \qquad (2)$$

Where $x(i,j)$ is represents the pixel values of originalvideo frame and$y(i, j)$represents the corresponding pixel values of watermarked frame and i and j are the pixelposition of the M×N video frame.
MSE is zero when $x(i, j) = y(i, j)$

3.2.1.2 Peak signal to noise ratio (PSNR)

The PSNR is evaluated in decibels and is inversely proportional the Mean Squared Error. It is given by the equation

$$PSNR = 10\log_{10}\frac{255}{\sqrt{MSE}} \qquad (3)$$

Higher the value of PSNR better is the quality of the watermarked frame.

3.2.1.3 Bit error rate (BER)

BER is the reciprocal of the PSNR.

$$BER = \frac{1}{PSNR} \qquad (4)$$

The value of BER which is closer to zero represents more quality of the watermarked frame.

3.2.2 Security

Securitydescribes if the embedded watermarking information cannot be removed beyond reliable detection.

3.2.3 Complexity

Complexitydescribes the effort and time we need for watermark embedding and retrieval video. Another aspect addresses if we need the original data in the retrieval process or not i.e. the watermarking algorithm is non-blind or blind which influence the complexity.

3.2.4 Capacity/Payload

Itdescribes how many information bits can be embedded.

3.2.5 Robustness

Robustnessdescribes if the watermark can be reliably extracted from the watermarked video [3, 5]. We can say Robustness of a watermarking algorithm is a measure of the immunity or resistance of the watermark against attempts to remove or degrade it from the video manipulations by different types of digital signal processing attacks. The similarity between the original watermark and the extracted watermark from the watermarked video can be measured by using the correlation factor ρ, which is computed using the following Equation:

$$\rho(W_o, W_r) = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} W_{oij} * W_{rij}}{\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N} W_{oij}^{\,2}}\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N} W_{rij}^{\,2}}} \qquad (5)$$

Where W_{oij} is a pixel of original watermark and W_{rij} is a pixel of the recovered watermark of size M X N.

The correlation factor $\boldsymbol{\rho}$ may take values between 0 and1. The value closer to 1 represents the more similarity between the original watermark and extracted watermark.

IV. PROPOSED ALGORITHM

In proposed algorithm, the input video sequence is divided into its constituted frames. Then 10 random frames are selected through the functions generated using a secret key entered by owner of the video. Then theseselected framesare used to embed the watermark using Discrete Wavelet Transform (DWT). The embedding and extraction process of watermark is given in Figure 1. The embedding and extraction algorithm is given below in detail.

4.1 Watermark Embedding Algorithm

Step 1: Extract all the frames N from input video file.
Step 2: Enter 10 digit secret key for random frame selection where each digit of key is 8bit.
Step 3: Calculate an offset value using total number of frames in video for uniform selection of frames.

$$off = \frac{N}{10} \qquad (12)$$

Step 4: Using the ASCII values of 10 digits of the key entered in step 2 & offset value calculated in step 3 to generate 10 random functions to select 10 random frames from the video for watermarking.If the digits of key are a, b, c, d, e, f, g, h, i, j then the 10 functions will be

$$x1 = (off * 0) + (a + b)$$
$$x2 = (off * 1) + (b + c)$$
$$x3 = (off * 2) + (c + d)$$
$$x4 = (off * 3) + (d + e)$$
$$x5 = (off * 4) + (e + f)$$
$$x6 = (off * 5) + (f + g)$$
$$x7 = (off * 6) + (h + h)$$
$$x8 = (off * 7) + (b + i)$$
$$x9 = (off * 8) + (g + h)$$

$x10 = (off * 9) + (b + d)$

If addition of ASCII values of two digits is greater than the offset value, then offset value is subtracted from their sum to get a number which is less than offset value.These 10 values of $x1$ to $x10$ represent the frame numbers. Frames with these frame numbers are selected for watermarking.

Step 5: Select the blue component from the selected RGB frame in which the watermark is to be embedded.

Step 6: Apply discrete wavelet transform (DWT) to this blue component and get approximation, horizontal, vertical, and diagonal details A, H, V & D respectively.

Step 7: Rescale the watermark image as per the size of the diagonal details D.

Step 8: The watermark (W matrix) is added to the diagonal details (D matrix) and get watermarked diagonal details (Dw)Dw = D + kW

Where k is the scale factor that controls the strength of the watermark embedded to the original image.

Step 10: The watermarked blue component is obtained by applying the inverse DWT using original approximation A, horizontal details H, vertical details V, and watermarked diagonal details Dw.

Step 11: Integrate this modified blue component with red and green components to get the watermarked RGB Frame.

Step 12: Repeat step 5 to step 11 for all the selected frames for watermarking to get the watermarked frames.

Step 13: Generate the checksum from the key used in step 2 and store the checksum into the red component of frame 1. Set the first pixel value to zero in the red component of frame 2.

Step 14: Develop the watermarked video using the modified frames by placing them to their respective position.

4.2 Watermark Extraction Algorithm

Step 1: Extract all the N frames from watermarked video file.

Step 2: Ask the user to enter the secret key.

Step 3: Generate the checksum from the key entered by the user in step 2.

Step 4: Extract the checksum of original key stored in the red component of frame 1.

Step 5: Compare both the checksums from step 3 & step 4. And increment the first pixel value in the red component of frame 2 every time checksum goes wrong.

Step 6: When this pixel value reaches four then corrupt the video file by writing zero to all pixel values of video. And stop the extraction process.

Step 7: If checksum matches then use the key entered in step 2 for finding the watermarked frames in the video. Follow step 4 of embedding process to find the watermarked frames.

Step 8: Select the blue component of watermarked frame from which the watermark is to be extracted.

Step 9: Apply DWT to this blue component and get approximation, horizontal, vertical, and watermarked diagonal details Dw respectively.

Step 10: Extract the watermark matrix from the Dw using the

W' = (Dw – D)/k

V. EXPERIMENTAL RESULTS AND PERFORMANCE EVALUATION

MATLAB 7.10.0 is used as the platform for implementing the proposed work & conducting experiments. The performance of the proposed video watermarking algorithm is evaluated using many colored videos containing different number of frames at various frame rates. But here results are discussed for a 8 seconds video clip of "traffic" at a frame rate of 15fps constituting of 120 frames. The watermark used in our experiments was a grayscale image of size 256 X 256. Secret key used is "Pavneet@12" based on which random frames are selected. A video frame, watermark image & corresponding watermarked frame is shown in figure 2.

a

b

c

Figure 2: (a) Original Video Frame(b) Watermark Image (c) Watermarked Frame

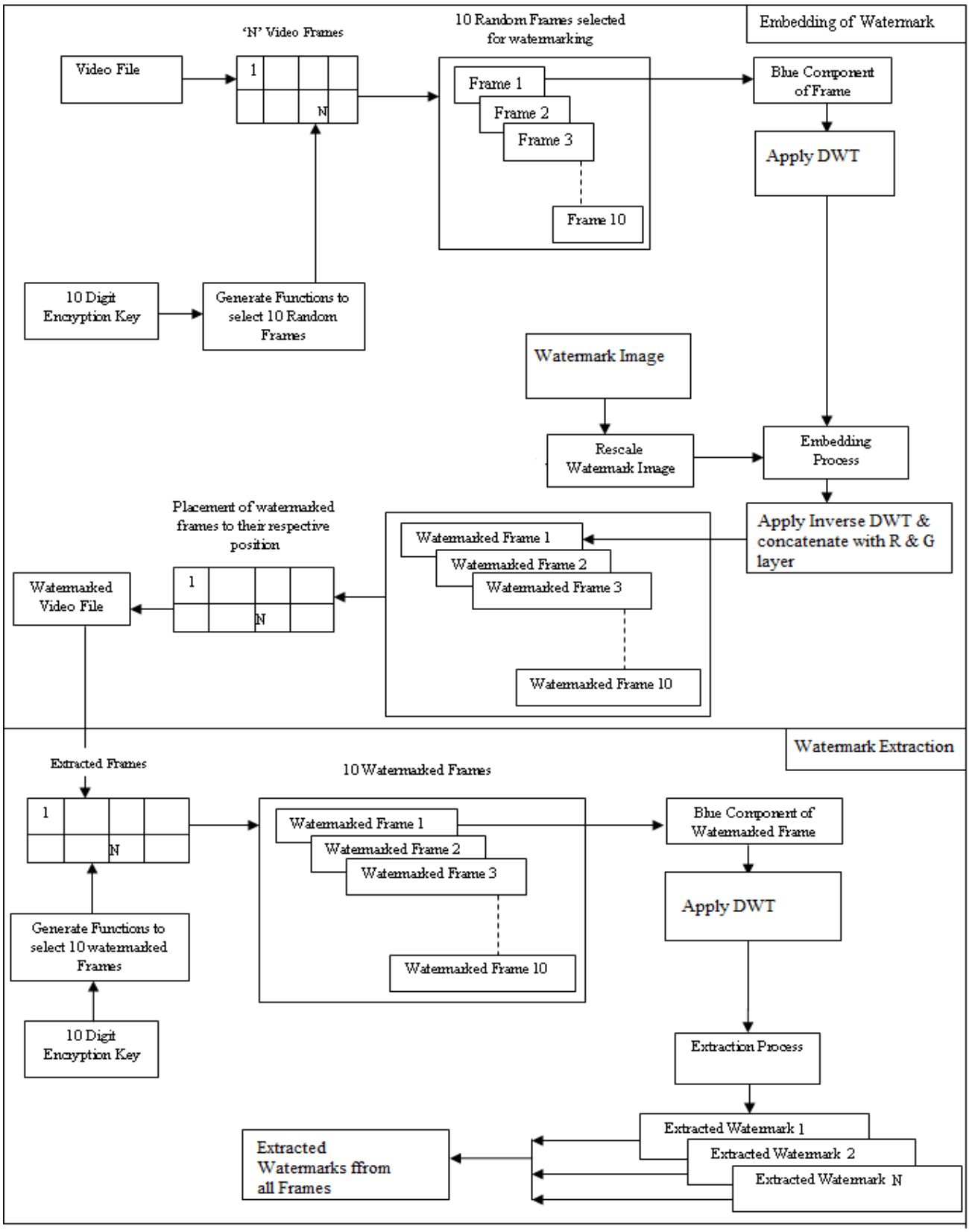


Figure 1: Watermark Embedding and Extraction Process

5.1 Imperceptibility performance:

To prove the proposed algorithm imperceptible, as a measure of quality of the watermarked video Mean Squared Error (MSE), Peak Signal to Noise Ratio (PSNR), and Bit Error Rate (BER) is calculated using equations (2), (3), (4) respectively for all the watermarked frames. The values for these parameters for all the frames & their average values are tabulated in table 1. Figure3, 4, 5 shows the values of MSE, PSNR, and BER respectively for all the watermarked frames.Higher average value of PSNR (59.4364 dB), smaller values of MSE (0.0740), and BER (0.0168) shows the imperceptibility of proposed algorithm.

5.2 Security

The proposed algorithm is more secure than the conventional algorithms due to the use of ansecret key for the selection of the frames to be watermarked. And at time of extraction process same encryption key is needed and if key is wrong then nobody can find the watermarked frames. And if someone tries for extraction with wrong key then he will be given only three chances of extraction, after that watermarked video will be damaged due to illegal processing and video will be of no use for that person.

5.3 Complexity

The proposed algorithm is very simple and semi blind algorithm.

5.4 Embedding Time:

Time consumed by the proposed watermarking algorithm is very small and is independent of the total video time because the frames to be watermarked are fixed. In proposed algorithm we are selecting 10 frames for watermarking. The considered video of “traffic” is of 8 seconds. The frame extraction time is 5.01 seconds, frame reassembling time is 5.01 seconds and time consumed for watermarking of 10 frames is 4.25 seconds so total time consumed for whole embedding process is 14.27 seconds. If the video size is increased then the frame extraction & frame reassembling time increases but the watermarking time remains same which is approximately 4-10 seconds.

5.5 Data Payload

In proposed algorithm, watermark of size half the size of the frame can be embedded into the video. Experiments are performed on a frame size of 512 X 512. So a watermark of size 256 X 256 can be embedded.

5.6 RobustnessPerformance

Similarity between the original watermark and the extracted watermarks from all the watermarked video frames is measured by computing correlation factor ρ using the equation (5). Random watermarked frame numbers are listed in table 1 & the extracted watermarks from respective frames are shown in figure 8. Original watermark & their correlation factor is also shown in figure 8.

The proposed algorithm is more robust to frame dropping as well as other attacks than the conventional methods. Because to destroy the watermark from watermarked frames, the watermark frames should be known. And the watermarked frames cannot be found out easily due to random & uniform frame selection for watermarking using the encryption key. Watermark is not embedded in the frames of one chunk but it is spread uniformly throughout the video to avoid the clustering of watermarked frames in one chunk. Also in proposed algorithm same watermark image is embedded in all the frames due to which if watermark is destroyed in some watermarked frames by any manipulation or some watermarked frames are dropped then it can be recovered from the others and probability of maintaining the watermark in manipulated watermarked video increases.

The Proposed algorithm is robust to various attacks like “poisson” noise attack and “Salt & pepper” noise attack as shown in figures 7 -10.

Table 1: Values of MSE, PSNR, BERfor all the Frames & their average

Watermarked Frame	**Frame 1**	**Frame 2**	**Frame 3**	**Frame 4**	**Frame 5**	**Frame 6**	**Frame 7**	**Frame 8**	**Frame 9**	**Frame 10**	**Average Value**
Random Frame Number	9	23	36	43	58	61	80	86	108	111	**NA**
MSE	0.074086	0.073656	0.074079	0.074086	0.074086	0.074086	0.074085	0.074086	0.074081	0.074021	**0.0740**
PSNR	59.4335	59.4587	59.4338	59.4335	59.4335	59.4335	59.4335	59.4335	59.4337	59.4373	**59.4364**
BER	0.016826	0.016818	0.016825	0.016826	0.016826	0.016826	0.016826	0.016826	0.016825	0.016824	**0.0168**

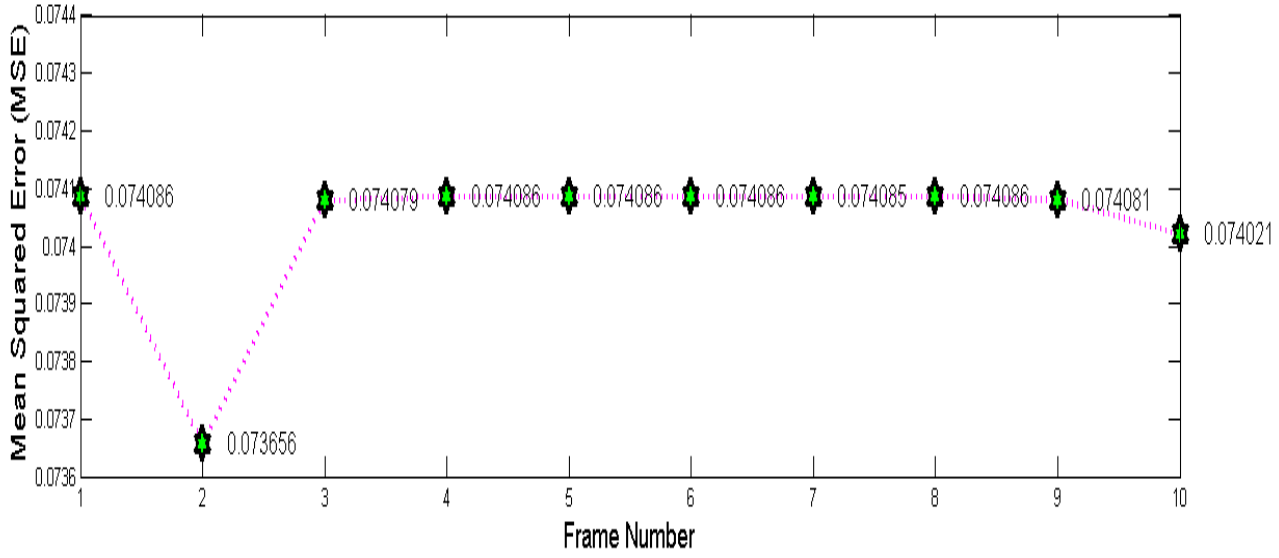


Figure 3: MSE Values for all the watermarked frames

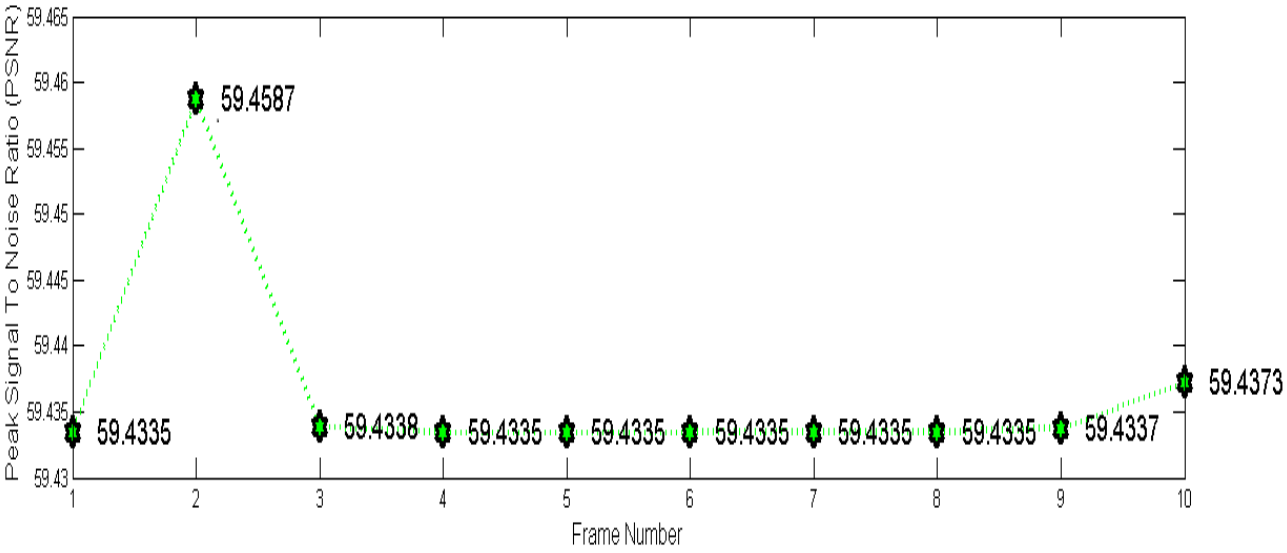


Figure 4: PSNR Values for all the watermarked frames

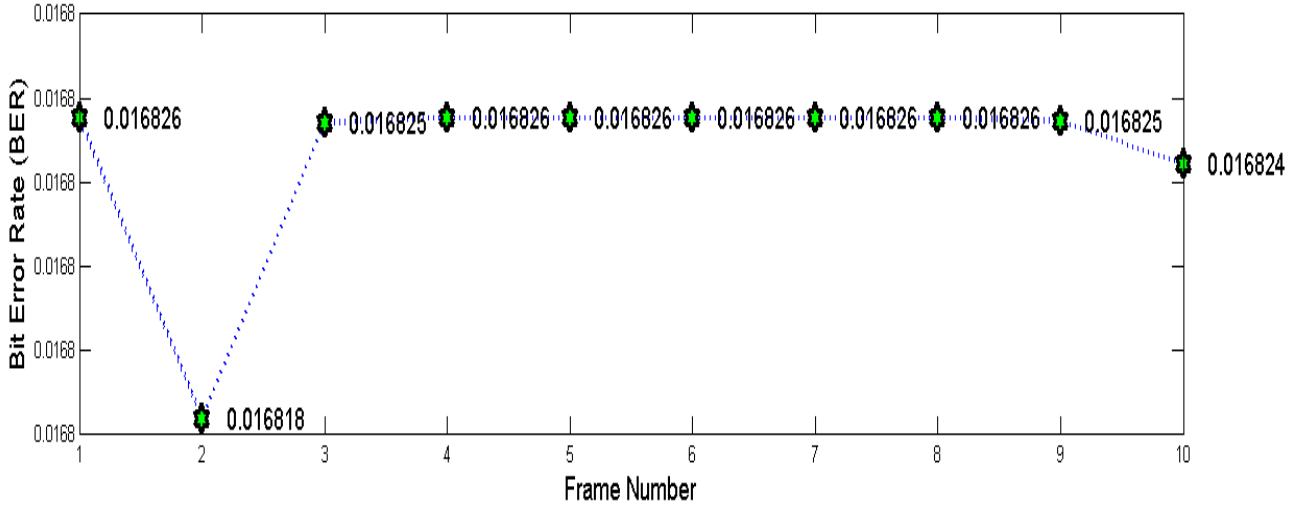


Figure 5: BER Values for all the watermarked frames

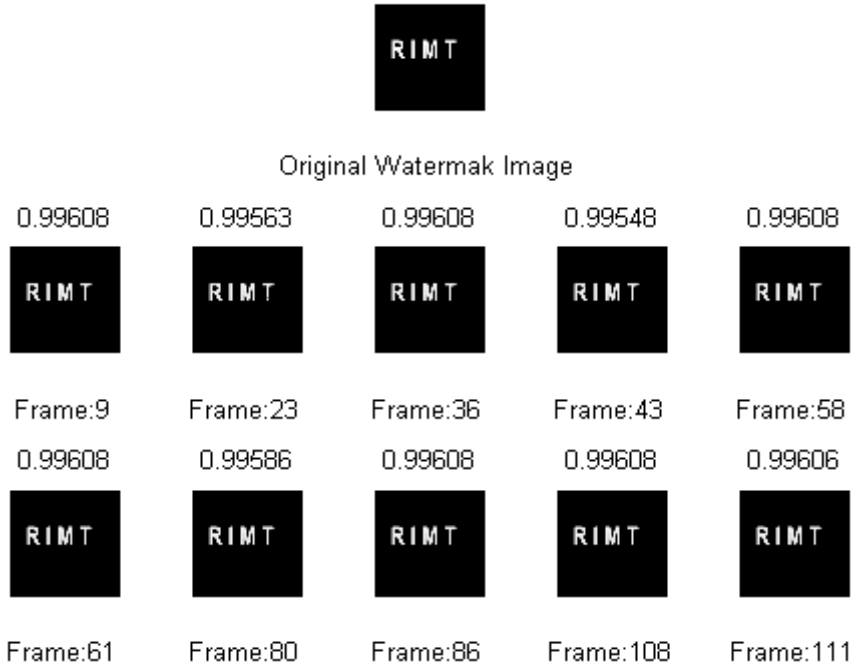


Figure 6: original watermark, extracted watermarks from all the 10 watermarked frames with frame number & their correlation factors

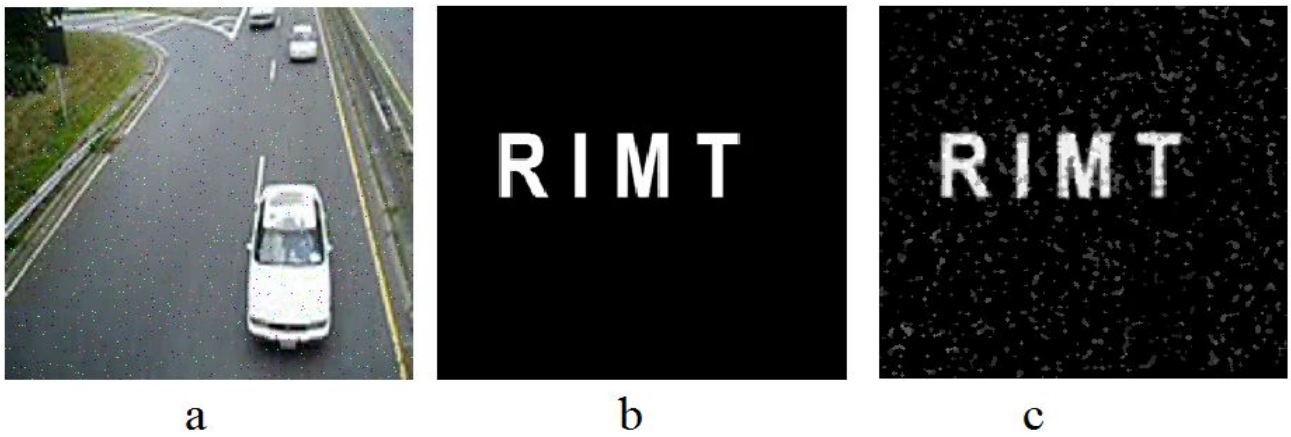


Figure 7 (a) salt & pepper noise Attacked frame (b) Original watermark (c) Extracted watermark (CC: 0.9054)

Figure 8: Extracted watermarks– After salt & pepper noise attack

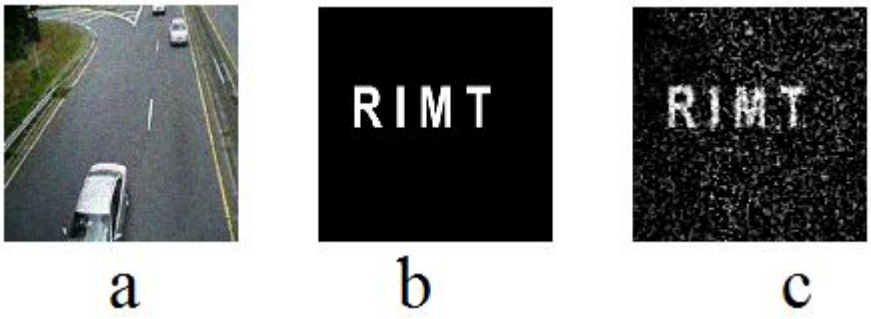


Figure 9(a) poisson noise Attacked frame (b) Original watermark (c) Extracted watermark (CC: 0.7049)

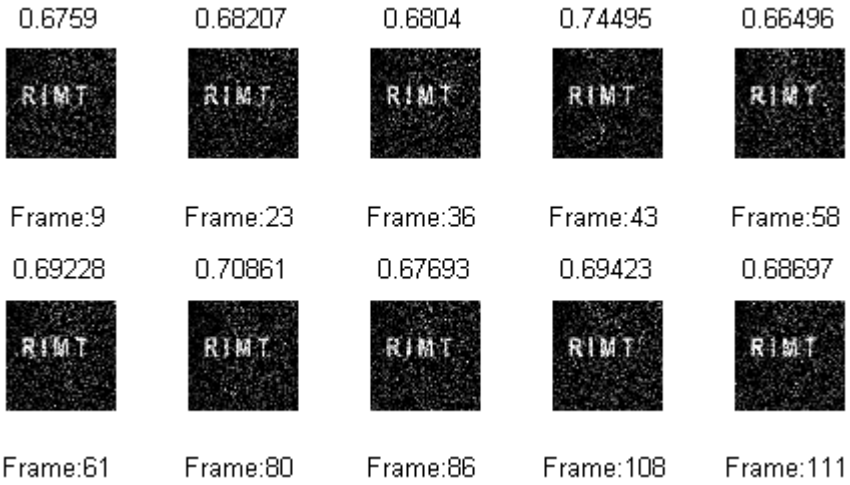


Figure 10: Extracted watermarks– After poisson noise attack

VI. CONCLUSIONS

In this paper, a blind video watermarking algorithm is proposed in which random frames from the whole video frames are selected for watermarking using an encryption key.To preserve the quality of the video, a particular selected frame is divided into blocks and the blocks of high entropies are selected for watermarking. Then watermark information is embedded at LSB of each pixel of the selected block. The algorithm is evaluated in terms of imperceptibility, security, time consumption, data payload and robustness. To measure the imperceptibility of algorithm PSNR, MSE, and BER are computed. The calculated values of these parameters show the high imperceptibility of the algorithm. Also the algorithm is simple semi blind algorithm, less time consuming, more secure and highly robust against various manipulations like frame dropping and noises.

REFERENCES

[1] L. Qiao and K. Nahrstedt, "Watermarking Schemes and Protocols For Protecting Rightful Ownership and Customer's Rights", Journal of Visual Commun. and Image Represent 9, pp.194– 210, 1998.

[2] M. Arnold, M. Schumucker, and S. Wolthusen, “Techniques and Applications of Digital Watermarking and Content Protection”. Artech House, 2003.

[3] Lama Rajab, Tahani Al-Khatib, Ali Al-Haj,“Video Watermarking Algorithms Using the SVD Transform” European Journal of Scientific Research, Vol.30 No.3, pp.389-401, 2009.

[4] Manekandan. GRS, Franklin Rajkumar. V, “A Robust Watermarking Scheme for Digital Video Sequence using Entropy and Hadamard Transformation Technique”, International Journal of Computer Applications, Volume 41– No.18,pp.24-31, March 2012.

[5] AngshumiSarma, Amrita Ganguly, “An Entropy based Video Watermarking Scheme”, International Journal of Computer Applications, Volume 50 – No.7, pp.24-31, July 2012.

[6] JigarMadia, Kapil Dave, VivekSampat, ParagToprani, “Video Watermarking using Dynamic Frame Selection Technique”, National Conference on Advancement of Technologies – Information Systems & Computer Networks (ISCON – 2012), pp.31-34, 2012.

[7] JassimMohmmed Ahmed, ZulkarnainMd Ali, “Information Hiding using LSB technique”, International Journal of Computer Science and Network Security, VOL.11 No.4, pp.18-25, April 2011.

[8] C.Sasivarnan, A.Jagan, JaspreetKaur, DivyaJyoti, Dr.D.S.Rao, “Image Quality Assessment Techniques on Spatial Domain”, IJCST Vol. 2, Issue 3, pp. 177-184, September 2011