A Bit Level and Entropy based Blind Watermarking Scheme for Video Sequence using Random Frame Selection

Ankush Gawri
Electronics & Communication Engineering
Guru Teg Bahadur Khalsa Institute of Engineering & Technology, Malout, Punjab, India

Sukhjit Singh
Electronics & Communication Engineering
Guru Teg Bahadur Khalsa Institute of Engineering & Technology, Malout, Punjab, India

ABSTRACT
Digital video watermarking 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 only few blocks on the basis of higher entropy are selected and watermarked using LSB technique. The performance of algorithm is tested using MATLAB software on video of "rhinos" and watermark image of 512 X 512. The experimental results show that the proposed scheme is highly imperceptible, less time consuming, more secure and highly robust against frame dropping & other manipulations.

General Terms
Digital Watermarking, Security, Imperceptibility, Robustness

Keywords
Video Watermarking, Entropy, PSNR, MSE, BER, SSIM

1. 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 against frame dropping & more secure scheme due to use of encryption key and random frame selection.

2. PROBLEM STATEMENT
As digital video-based application technologies grow, such as Internet video, wireless video, Video phones, and video conferencing, the problem of illegal manipulation, copying, distribution and piracy of digital video 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 encryption key.

The watermark is embedded in these selected frames. Encryption key used is decided by the owner of the video. And the random frames are selected by using the functions generated through this authentication key. These functions are designed such that avoiding the selection/clustering of frames in one chunk. Instead of the clustering of frames, the frames are selected uniformly from whole video. Then same watermark information is used to embed in all the selected frames to increase the probability of maintaining the watermark in manipulated watermarked video. For example if some unauthorized person tries to drop some frames of the video, then if some watermarked frames dropped from the video, and if only one watermarked frame is left behind in the video then the watermark information can be recovered from this frame only. The manipulations can be done with video either through frame dropping or through any other way by any unauthorized person for illegal copying the video. To preserve the quality of the video & keep the algorithm more imperceptible the entire video frame is not altered by embedding the watermark information. Instead of that the frame is divided into blocks of 8 X 8. And only few selected blocks are used to embed the watermark information. To select these blocks the concept of entropy is used. Blocks of higher entropy are selected for watermarking because if watermark is embedded in high entropy areas of an image or video frame then higher imperceptibility can be obtained. And watermark information is embedded in the selected frames at bit level. Least significant bit (LSB) of each pixel value of selected block is replaced by the one bit information of watermark pattern [7]. After watermarking the frames, we

insert them back in the video at their respective places to get the watermarked video.

To extract the watermark from watermarked frames again same encryption key is required to find the watermarked frames. We set up a key identifier to give only three trials to the user. If the use tries extraction with more than 3 wrong keys then it is assumed that he is trying to find the watermarked frames by trying random keys. So at fourth try with wrong key the video is corrupted leaving no data behind.

3. 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 Entropy

There are many ways with which texture of multidimensional frame could be measured. Entropy is most suitable way to measure the texture content of an image or a video frame. Texture provides measures of properties of a frame such as smoothness, coarseness and regularity. Higher the entropy, least will be that part visible to human because human eye is insensitive to these high entropy areas. Hence, if watermark is embedded in high entropy areas of an image or video frame then higher imperceptibility can be obtained. Entropy is a statistical measure of randomness that can be used to characterize the texture of the input image or video frame. Let P contains the histogram counts. The entropy is represented as

$$E = -\sum P \log_2(P) \qquad (1)$$

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 to Noise Ratio (PSNR), Mean Squared Error (MSE) and Structural Similarity Index Metric (SSIM) 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 watermarked frame 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 original video frame and *y*(*i, j*) represents the corresponding pixel values of watermarked frame and i and j are the pixel position of the M×N image.

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.

3.2.1.4 Structural Similarity Index Metric (SSIM)

The structural similarity (SSIM) index is a method for measuring the similarity between the original video frame and watermarked frame. The SSIM index is a full reference metric, in other words, the measuring of quality based on an initial distortion-free original frame as reference. The difference with respect to other techniques mentioned previously such as MSE or PSNR, is that these approaches estimate *perceived errors* on the other hand SSIM considers frame degradation as *perceived change in structural information*. Structural information is the idea that the pixels have strong inter-dependencies especially when they are spatially close. These dependencies carry important information about the structure of the objects in the visual scene.

The SSIM metric is calculated on various windows of any frame. The measure between two windows x and y of common size $N \times N$ is:

$$SSIM(x,y) = \frac{(2\bar{x}\bar{y} + C1)(2\sigma_{xy} + C2)}{((\bar{x})^2 + (\bar{y}^2) + C1)(\sigma_x{}^2 + \sigma_y{}^2 + C2)} \qquad (5)$$

Where C1 & C2 are constants. $\bar{x}, \bar{y}, \sigma_x{}^2, \sigma_y{}^2$ *and* σ_{xy} are given as:

$$\bar{x} = \frac{1}{N}\sum_{i=1}^{N} x_i \qquad (6)$$

$$\bar{y} = \frac{1}{N}\sum_{i=1}^{N} y_i \qquad (7)$$

$$\sigma_x{}^2 = \frac{1}{N-1}\sum_{i=1}^{N}(x - \bar{x})^2 \qquad (8)$$

$$\sigma_y{}^2 = \frac{1}{N-1}\sum_{i=1}^{N}(y - \bar{y})^2 \qquad (9)$$

$$\sigma_{xy} = \frac{1}{N-1}\sum_{i=1}^{N}(x - \bar{x})(y - \bar{y}) \qquad (10)$$

SSIM value closer to 1 represents the better quality of watermarked video.

3.2.2 Security

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

3.2.3 Complexity

Complexity describes 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

It describes how many information bits can be embedded.

3.2.5 Robustness

Robustness describes 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:

$$\rho(w_o, w_r) = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} w_{oij} * w_{rij}}{\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N} w_{oij}{}^2}\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N} w_{rij}{}^2}} \quad (11)$$

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.

4. PROPOSED ALGORITHM

In our proposed algorithm, entropy concept is used for embedding watermark. And watermarking is performed at bit level. The input video sequence is divided into its constituted frames. Then 10 random frames are selected through the functions generated using encryption key entered by owner of the video. Then the frame to be watermarked is divided into blocks of 8 X 8 and entropy is calculated for each block. The blocks with higher entropies are selected for embedding watermark. 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 encryption 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.

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

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 number. 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: Divide the blue component into blocks B_{ij} of size 8X8. And find the entropy for each block and also find the threshold value.
Step 7: Select the 8 X 8 blocks B'_{ij} for watermarking whose entropy value is greater than threshold value
Step 8: Rescale the watermark image as per the count of the selected blocks so that the size of the watermark will match with the total size of selected blocks for embedding.
Step 9: Divide the watermark into the blocks W_{ij} of size 8X8
Step 10: Embed the watermark blocks $W_{ij}$from step 10 into the selected blocks B'_{ij} from step 7. For embedding replace the binary bits of the watermark block W_{ij} with the LSB of each corresponding pixel of block B'_{ij}. In all watermarked blocks replace any fixed position pixel value with zero.
Step 11: Rearrange these modified blocks at their respective position and integrate all 8 X 8 blocks to get watermarked blue component.
Step 12: Integrate this modified blue component with red and green components to get the watermarked RGB Frame.
Step 13: Repeat step 5 to step 12 for all the selected frames for watermarking to get the watermarked frames.
Step 14: Generate the checksum from the key used in step 2 and store the checksum bits into the random pixels of the red component of frame 1. Set the first pixel value to zero in the red component of frame 2.
Step 15: 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 frames N from watermarked video file.
Step 2: Ask the user to enter the encryption 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.

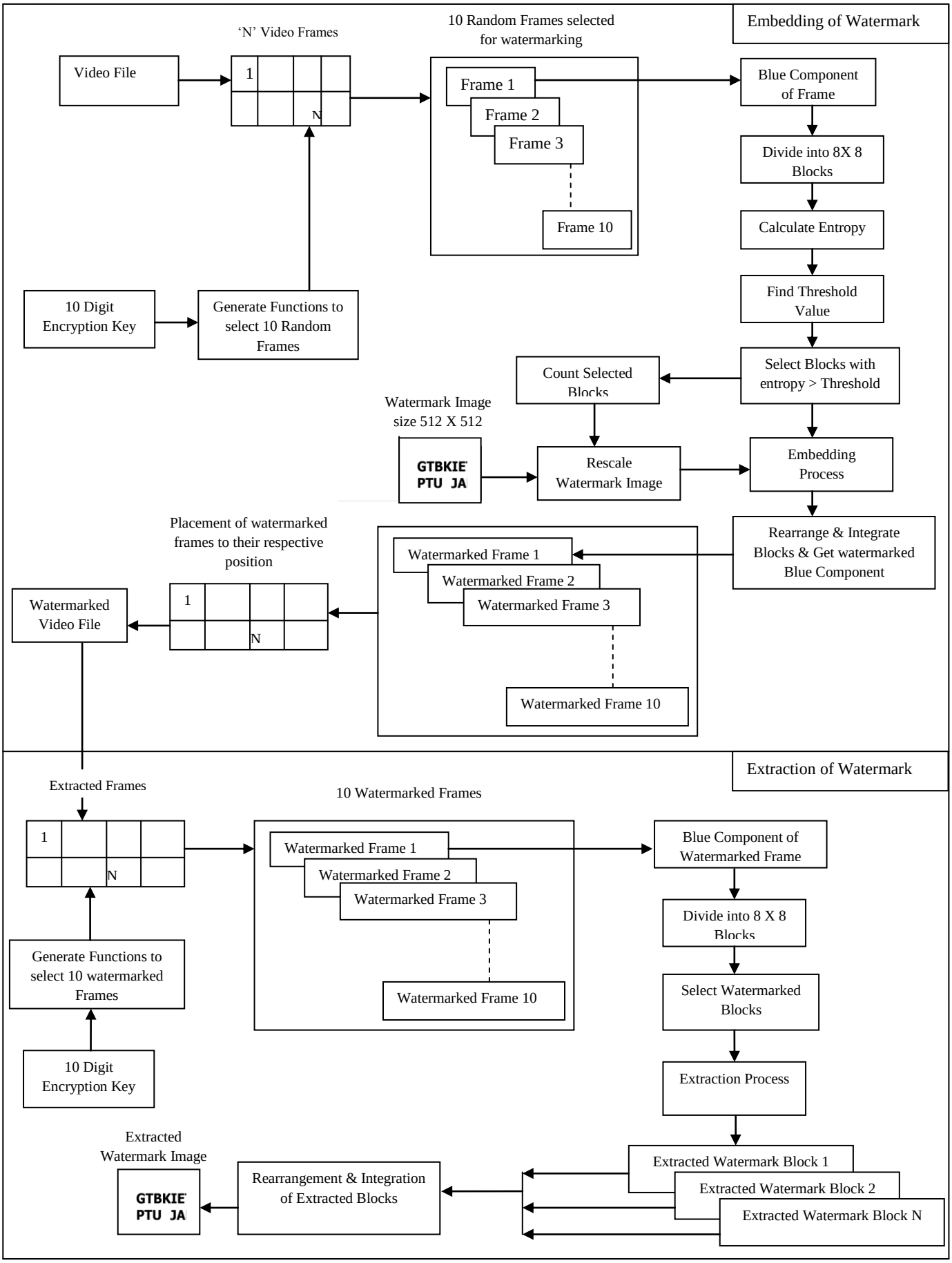

Figure 1: Watermark Embedding and Extraction Process

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: Divide the blue component into blocks of size 8 X 8.
Step 10: Out of these blocks select the watermarked blocks by checking zero in the fixed position pixel.
Step 11: Extract the watermark blocks from these watermarked blocks. Read the LSB of each pixel value of watermarked Block to extract the corresponding bit of watermark block.
Step 12: Rearrange all the extracted watermark blocks to get the extracted watermark image
Step 13: Rescale the extracted watermark image to the size of original watermark image

5. 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 7.6 seconds video clip of "rhinos" at a frame rate of 15fps constituting of 114 frames. The watermark used in our experiments was a binary image of 512 X 512. Encryption key used is "GAWRI@8146" based on which random frames are selected. A video frame, watermark image & corresponding watermarked frame is shown in figure 2.

Figure 2: Original Video Frame, Watermark Image & Watermarked Frame

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), Bit Error Rate (BER) and Structural Similarity Index Metric (SSIM) is calculated using equations (2), (3), (4), (5) respectively for all the watermarked frames. The values for these parameters for all the frames & their average values are tabulated in table 1. Figure 3, 4, 5, 6 shows the values of MSE, PSNR, BER and SSIM respectively for all the watermarked frames. Figure 7 shows the average values of these parameters. Higher average value of PSNR (64.57 dB), smaller values of MSE (0.0227) & BER (0.015) and value of SSIM (0.9583) closer to 1 shows the imperceptibility of proposed algorithm.

5.2 Security

The proposed algorithm is more secure than the conventional algorithms due to the use of an encryption 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 blind algorithm as for extracting process it doesn't require any original data to recover the watermark. And watermark can be extracted from only watermarked video.

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 "rhinos" is of 7.6 seconds. The frame extraction time is 6.60 seconds, frame reassembling time is 4.74 seconds and time consumed for watermarking of 10 frames is 24.57 seconds so total time consumed for whole embedding process is 35.91 seconds. If the video size is increased then the frame extraction & frame reassembling time increases but the watermarking time remains same which is approximately 25-30 seconds.

5.5 Data Payload

In proposed algorithm 8 X 8 blocks with high entropy are selected for watermark embedding. And one bit is embedded in one pixel i.e. total of 64 bits can be embedded in a selected blocks. Experiments are performed on a frame size of 512 X 512. So there are total 4096 blocks of a frame out of which minimum 2101 high entropy blocks are selected for data embedding and so minimum 1,34,464 bits can be embedded per frame.

5.6 Robustness Performance

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 (11). 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.

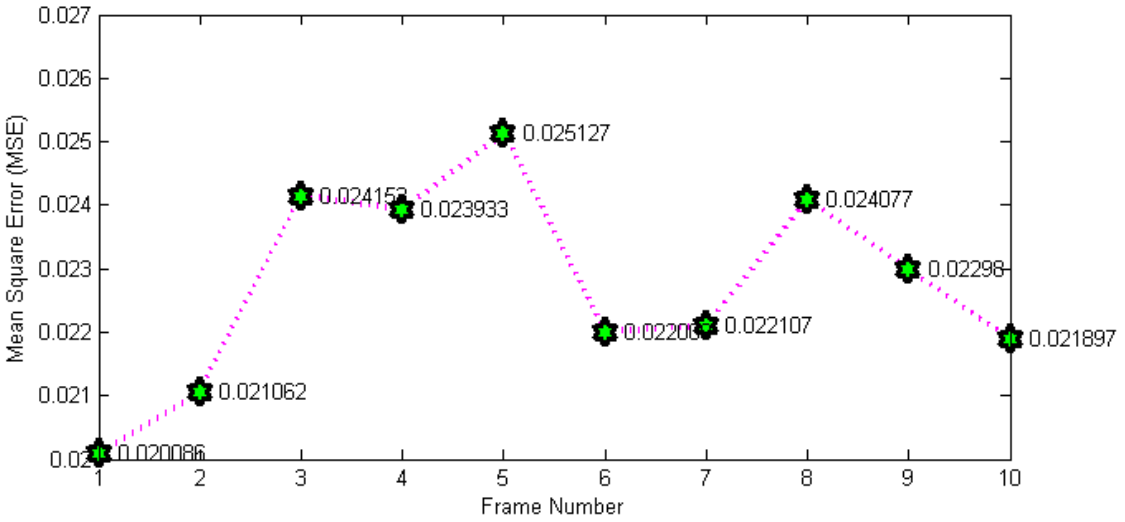

Figure 3: MSE Values for all the watermarked frames

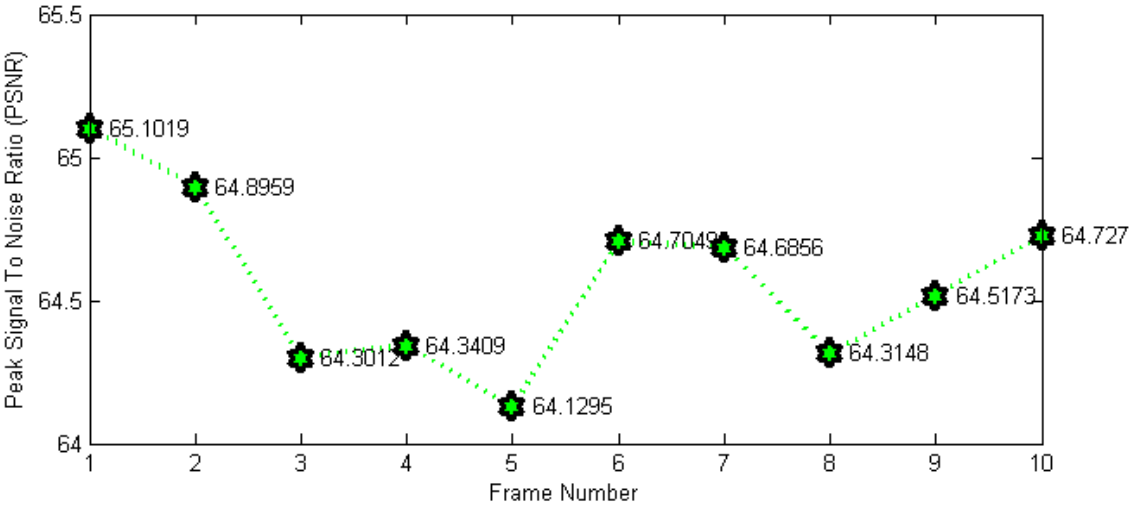

Figure 4: PSNR Values for all the watermarked frames

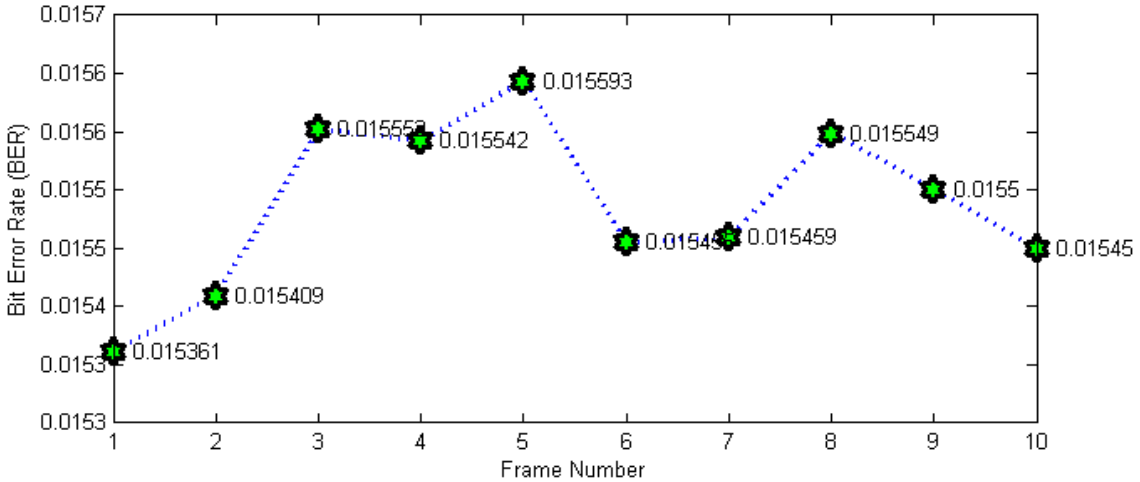

Figure 5: BER Values for all the watermarked frames

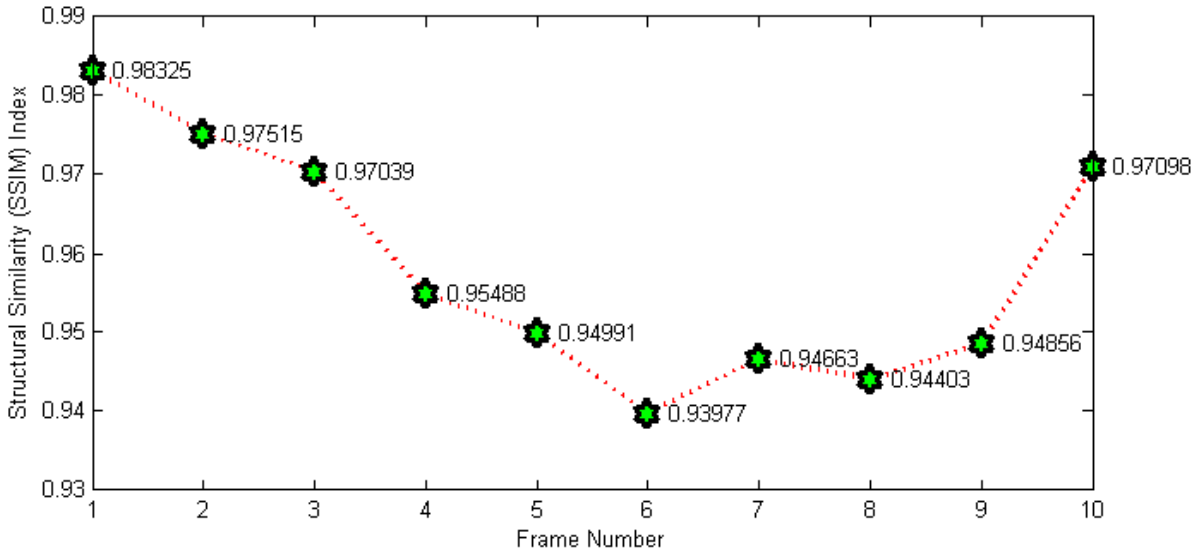

Figure 6: SSIM Values for all the watermarked frames

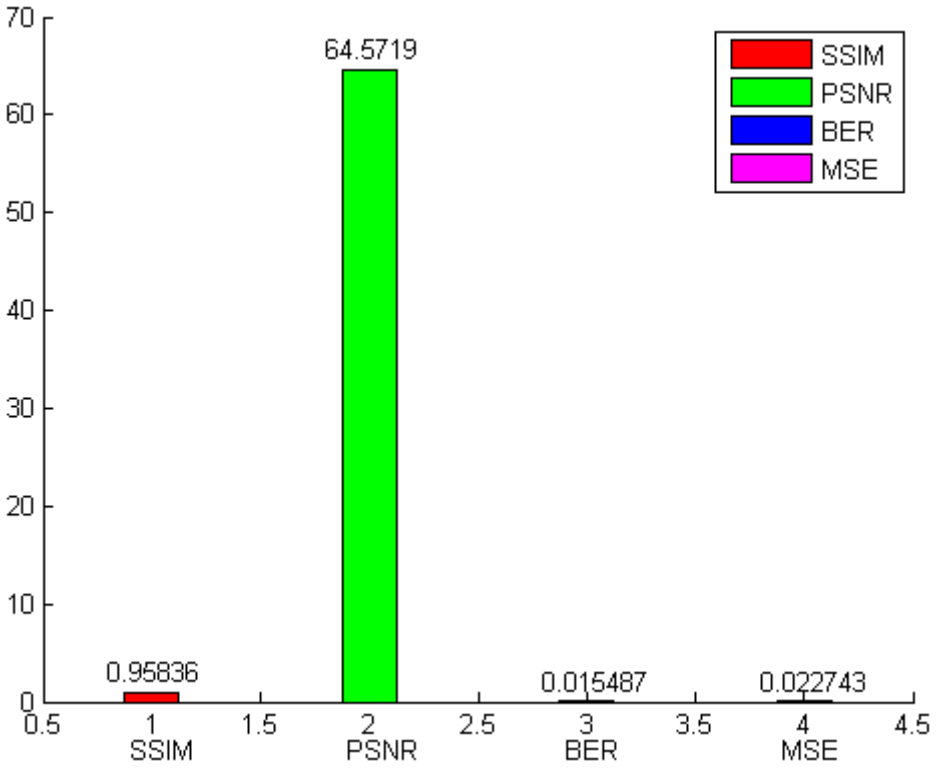

Figure 7: Average Values of PSNR, MSE, BER & SSIM of All the Frames

Table 1: Values of MSE, PSNR, BER, SSIM for 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	4	20	26	34	49	65	76	84	94	103	**NA**
MSE	0.020086	0.021062	0.024153	0.023933	0.025127	0.022009	0.022107	0.024077	0.02298	0.021897	**0.022743**
PSNR	65.1019	64.8959	64.3012	64.3409	64.1295	64.7049	64.6856	64.3148	64.5173	64.727	**64.5719**
BER	0.015361	0.015409	0.015552	0.015542	0.015593	0.015455	0.015459	0.015549	0.0155	0.01545	**0.015487**
SSIM	0.98325	0.97515	0.97039	0.95488	0.94991	0.93977	0.94663	0.94403	0.94856	0.97098	**0.95836**

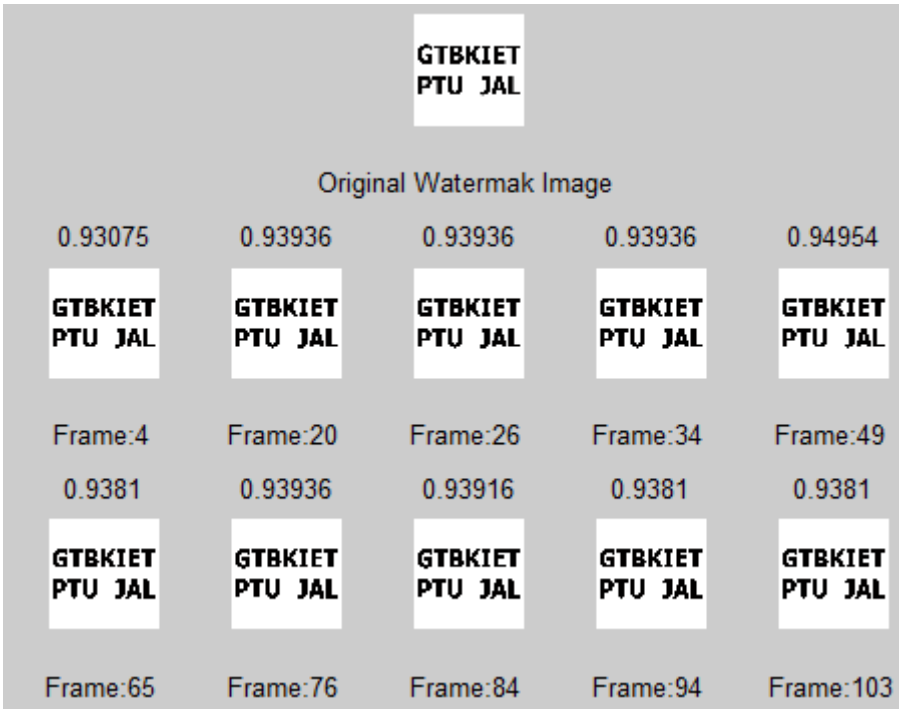

Figure 8: original watermark, extracted watermarks from all the 10 watermarked frames with frame number & their correlation factors

6. 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, BER & SSIM are computed. The calculated values of these parameters show the high imperceptibility of the algorithm. Also the algorithm is simple blind algorithm, less time consuming, more secure and highly robust against frame dropping & other manipulations.

7. 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] Angshumi Sarma, Amrita Ganguly, "An Entropy based Video Watermarking Scheme", International Journal of Computer Applications, Volume 50 – No.7, pp.24-31, July 2012.

[6] Jigar Madia, Kapil Dave, Vivek Sampat, Parag Toprani, "Video Watermarking using Dynamic Frame Selection Technique", National Conference on Advancement of Technologies – Information Systems & Computer Networks (ISCON – 2012), pp.31-34, 2012.

[7] Jassim Mohmmed Ahmed, Zulkarnain Md 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.Sasi varnan, A.Jagan, Jaspreet Kaur, Divya Jyoti, Dr.D.S.Rao, "Image Quality Assessment Techniques on Spatial Domain", IJCST Vol. 2, Issue 3, pp. 177-184, September 2011