Robust Video Watermarking Embedding & Extraction Algorithm using Discrete Wavelet Transform (DWT) Based on Random Frame Selection

Ekta¹ and Naresh Kumar Garg²

¹BFGI, Bathinda ²GZS PTU Campus, Bathinda E-mail: ¹ektanagpal.bfcmt@gmailcom, ²naresh2834@rediffmail.com

Abstract—Video watermarking is effectively a new technology that has been provided a platform to solve the problem of illegal manipulation and delivery of videos. In this paper, a highly robust and imperceptible video watermarking technique with the combination of a secret key technique to enhance the security of existing conventional watermarking techniques is projected. Rather than embedding the watermark in the all video frames only few frames are selected from the whole video sequence decided by the secret key. Secret key used is provided by the possessor of the video and the random frames are selected by using the functions generated with the help of secret key. Rather than bunch of frames, the frames are selected regularly from the complete video. In this projected approach, in the blue layer of each of the chosen frame, the watermark is embedded in the co-efficient matrix (horizontal) obtained using single level discrete 2-D wavelet function. First of all Decomposition wavelet is applied to extract horizontal component then reconstruction Wavelet is applied after embedding watermark in the horizontal co-efficient. Results show that the projected scheme guarantee high imperceptibility and robustness against various kinds of noise and other manipulations like rotation attacks.

Keywords: Video watermarking, DWT, Robustness, BER, PSNR, MSE, Secret Key.

1. INTRODUCTION

In recent years, cyberspace and compression technology permit the widespread use of multimedia applications. It is the process of embedding patent information in video bit streams. In this projected technique, an effective, imperceptible and robust video watermarking algorithm using Discrete Wavelet Transformation is projected. A watermark embedding technique is supplied with an un-watermarked video sequence and a binary message/watermark to embed in order to obtain a watermarked video sequence. This message can then be extracted using the appropriate watermark extraction technique and secret key. The performance of the projected algorithm is evaluated with respect to imperceptibility, robustness and data payload. This algorithm show high level of imperceptibility, robustness and payload. This paper presents a content-based digital video-watermarking scheme, which is robust against a variety of common image-processing attacks and geometric distortions.

1.1 Performance Metrices

In order to find the quality, imperceptibility and robustness of the watermarked video, quality measures parameters such as PSNR,MSE,BER are used.

The notions used are listed below.

X(i, j):Original video, Y(i, j): Watermarked and video, Nf : Size of video

1.2 Mean Square Error (MSE)

Mean Square Error between original video and watermarked video is calculated as follows:

$$MSE = \frac{1}{Nf} \sum_{i,j} [X(i,j) - Y(i,j)]^2$$

1.3 Peak Signal to Noise Ratio (PSNR)

PSNR is calculated between the original and watermarked video. Higher the PSNR value, more similar is watermarked video to the original video. The video quality metric is defined in decibels as:

$$PSNR = 10 \log_{10} \frac{255 * 255}{MSE}$$

1.4 Bit Error Rate (BER)

The performance metric is suitable for random binary sequence watermark. The parameter is defined as ratio between numbers of incorrectly decodes bits and length of the binary sequence. BER indicates probability of incorrectly decoded binary patterns. It is define as follows

$$BER = \frac{DB}{TB}$$

Where

DB: No. of incorrectly decoded bits, TB: Total no. of bits.

2. LITERATURE REVIEW

Schyndel et al. [6], (1994) changed the LSB of an image to embed a watermark. Since then, more and more researchers have studied digital watermarking problem.

Sinha et al. [5], (2011) projected a hybrid digital video watermarking scheme based on Discrete Wavelet Transform (DWT) and Principal Component Analysis (PCA). PCA helps in reducing correlation among the wavelet coefficients obtained from wavelet decomposition of each video frame thereby dispersing the watermark bits into the uncorrelated coefficients.

Sarma et al. [1], (2012) projected an entropy based blind video watermarking scheme using combined DCT-DWT transformation. 2level DWT was performed on the extracted video frames, which results in sixteen sub-bands.

Madia et al. [3], (2012) presented a novel video watermarking approach for frame selection in watermarking along with a combination that is both effective and secure, providing a very fine watermarking technique.

Bhatnagar et al. [2], (2009) described about how to decompose an image using MR-WHT (Multi-resolution Walsh-Hadamard Transform) and then middle singular values of High frequency sub-band at the finest and the coarsest level are modified with singular values of watermark.

Singh et al. [4], (2013) describes a bit level and entropy based blind video watermarking scheme based on random frame selection.

Anupma et al. [7], (2014) compare two well known algorithms of Video Watermarking- singular value decomposition and least significant bit and concluded SVD a better option.

3. PROJECTED ALGORITHM

In this projected algorithm, discrete wavelet transformation technique is used for embedding watermark. The input video sequence is divided into its constituted frames. Then 10 random frames are selected through the functions generated using secret key entered by owner of the video. Then to the frame to be watermarked discrete wavelet transformation technique has applied on these frames. The embedding and extraction algorithm is given below in detail and represented by fig. 1.

3.1 Watermark Embedding Algorithm

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

Step 2: Enter 10 digit secret key for random frame selection where each digit of key is 8 bit.

Step 3: Calculate a counteract value using N total number of frames in video for uniform selection of frames.

$$cou = \frac{N}{10}$$

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

$$x1 = (cou * 0) + (a + b)$$

$$x2 = (cou * 1) + (b + c)$$

$$x3 = (cou * 2) + (c + d)$$

$$x4 = (cou * 3) + (d + e)$$

$$x5 = (cou * 4) + (e + f)$$

$$x6 = (cou * 5) + (f + g)$$

$$x7 = (cou * 6) + (h + h)$$

$$x8 = (cou * 7) + (b + i)$$

$$x9 = (cou * 8) + (g + h)$$

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

If addition of ASCII values of two digits is greater than the counteract value, then counteract value is subtracted from their sum to get a number which is less than counteract 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 values of components of blue layer from the selected RGB frame in which the watermark is to be embedded.

Step 6: If the watermark is not the gray scale image, it is converted to gray scale.

Step7: Discrete wavelet transformation (DWT2) is applied to component selected at step 5 using Daubechies wavelet to extract all four co-efficient matrices-approximation, horizontal, vertical and diagonal

[A H V D]=dwt2(img,'db1')

Step 8: Watermark obtained at step 6 is embedded in the horizontal co-efficient matrices obtained at step 8 with intensity k.

Hw=H+k*gray-watermark

Step 9: Reconstruction wavelet function is applied using new horizontal co-efficient matrices obtained at step 8.

Watermarked_video_frame=idwt2(A,Hw,V,D,'db')

Step 10: Integrate this modified blue component with red and green components to get the watermarked RGB Frame.

Step 11: Repeat step 5 to step 10 for all the selected frames for watermarking to get the watermarked frames.

Step 12: Store the secret key used in step 2 into the random pixels of the red component of frame 1. Put the first pixel value to zero in the red component of frame 2.

Step 13: Develop the watermarked video using the customized frames by placing them to their respective position.

3.2 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: Extract the original secret key stored in the red component of frame 1.

Step 5: Compare both the secret keys from step 3 & step 4. And increment the first pixel value in the red component of frame 2 every time comparison 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 secret key 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 components of blue layer from the RGB watermarked frame from which the watermark is to be extracted.

Step 9: Discrete wavelet transformation (DWT2) is applied to component selected at step 8 using Daubechies wavelet to extract all four co-efficient matrices-approximation, horizontal, vertical and diagonal from the blue component of watermarked video frame

[A Hw V D]=dwt2(watermarked-frame,'db1')

Step 10: Watermark is extracted by using Original horizontal co-efficient matrices, watermarked horizontal co-efficient matrices & k intensity factor.

Extracted-Videowatermark=(Hw-H)/K

Step11: Apply the same process to extract watermark from all the watermarked frames from step 8 to step 10.

Step 12: Rescale the extracted watermark image to the size of original watermark image.

4. **RESULTS AND DISCUSSION**

A novel approach described in previous section for video watermarking is implemented and experiments are conducted for watermark embedding and extraction using MATLAB 7.10.0 version. The performance of the projected video watermarking algorithm is evaluated on the base of security, Imperceptibility, complexity, robustness, and embedding time. The performance of the projected 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 07 seconds duration video clip of "rhinos" at a frame rate of 15frames/sec constituting of 105 frames. Secret key used is "ektanagpal" based on which 10 random frames from the video are selected for watermarking. The watermark used in our experiments was a binary image of 256 X 256 pixels as shown in Fig. 2. This watermark image is used to embed in each of the selected 10 frames. Ten random frames out of total no. of frames selected from the video to be watermarked and the selected frame numbers are Frames number 10,14,26,42,53,57,70,83,94,105 & corresponding watermarked frames are shown in Fig. 2.



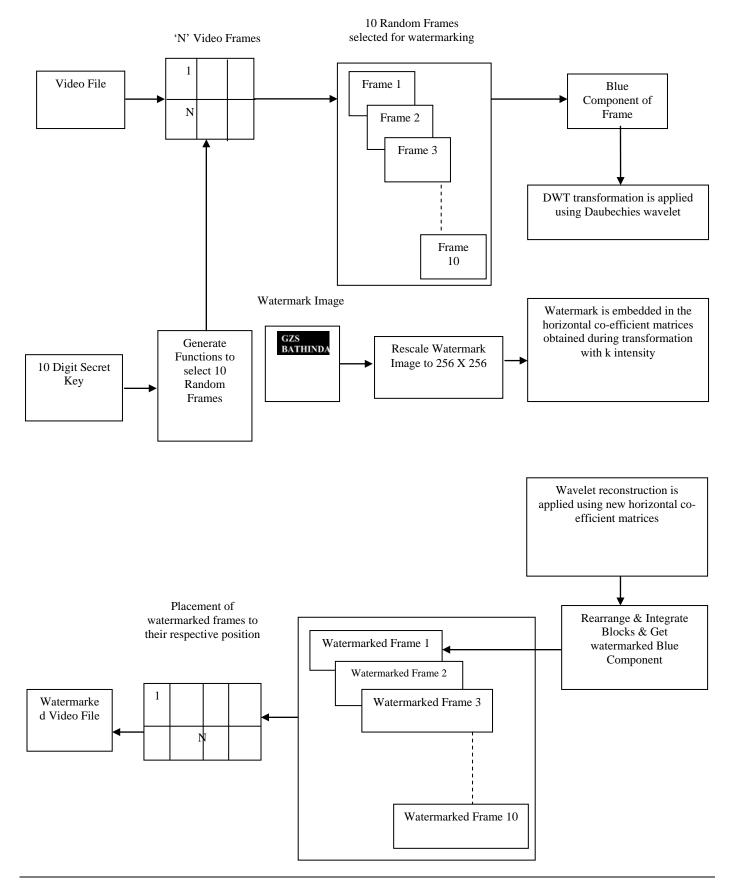


Fig. 2: Original video frame, Watermark Image & Watermarked frame

The algorithm performance is discussed in following sections.

4.1 Imperceptibility Performance

To prove the projected algorithm imperceptible, as a determine of quality of the watermarked video Mean Squared Error (MSE), Peak Signal to Noise Ratio (PSNR) and Bit Error Rate (BER) is calculated for all the watermarked frames. The values for these parameters for all the frames are tabulated in table 1. Higher average value of PSNR (58.27828 dB), smaller values of MSE (0.0965583) & BER (0.0171543) shows that the projected algorithm is highly imperceptible.



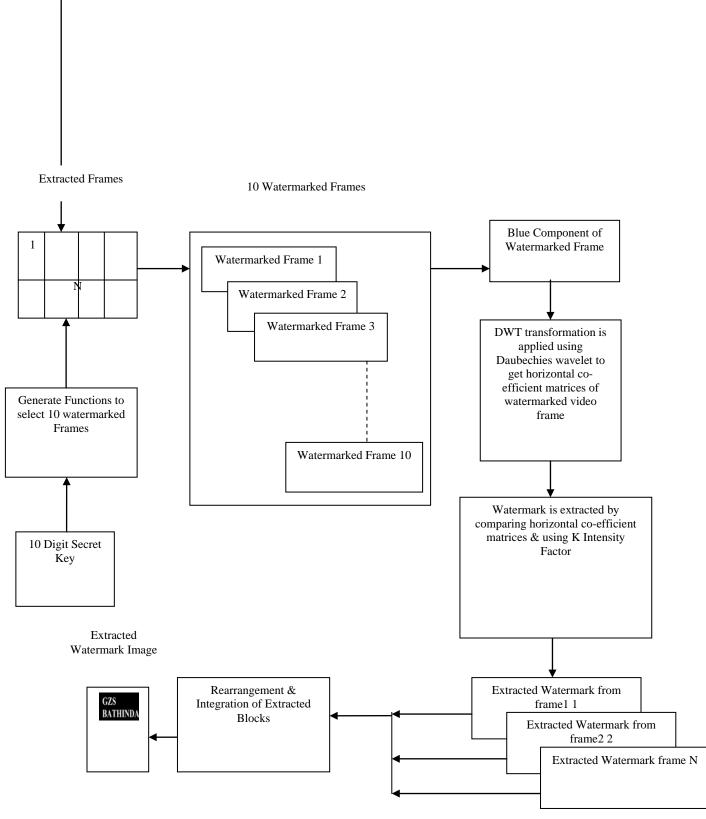


Fig. 1: Block Diagram of Projected Video Watermark Embedding and Extraction Process

Random Selected Frame	MSE	PSNR	BER
Frame number 10	0.097325	58.24	0.01716
Frame number 14	0.097108	58.25	0.017168
Frame number 26	0.097320	58.24	0.017160
Frame number 42	0.097220	58.24	0.017160
Frame number 53	0.097230	58.24	0.017168
Frame number 57	0.097332	58.2483	0.01716
Frame number 70	0.096696	58.2767	0.01716
Frame number 83	0.092268	58.4803	0.0171
Frame number 94	0.095754	58.3192	0.017147
Frame number 105	0.09733	58.2483	0.01716
Average Value	0.0965583	58.27828	0.0171543

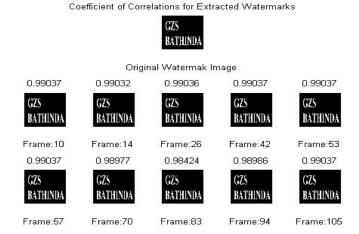
Table 1: Values of Quality Parameters MSE, PSNR &BER by using Projected Technique

4.2 Security

The projected algorithm is more secure than the conventional algorithms due to the use of the secret key for the selection of the frames to be watermarked. And at time of extraction process same secret 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/she 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.

4.3 Robustness Performance

Similarity between the original watermark and the extracted watermarks from all the watermarked video frames is measured by computing correlation factor ρ . Original watermark and extracted watermarks from the watermarked video are shown in the Fig. 3 and after applying various kinds of noise attacks the obtained correlation factors are tabulated in Table2.



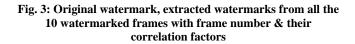


Table 2: Correlation factor of each extracted watermark after	
applying various attacks	

Watermark Extracted from	Correlation factor (ρ)	Correlation factor (ρ)	Correlation factor (p)
Extracted from	(After	(After	(After adding
	adding	adding	salt& Pepper
	Gaussian	Poisson	Noise)
	Noise)	Noise)	
Frame number 10	0.7704	0.6809	0.89414
Frame number 14	0.7638	0.66417	0.89116
Frame number 26	0.77591	0.69847	0.88313
Frame number 42	0.77027	0.62406	0.90597
Frame number 53	0.76716	0.62542	0.91069
Frame number 57	0.77215	0.60518	0.90914
Frame number 70	0.77582	0.61703	0.90265
Frame number 83	0.76719	0.61862	0.87955
Frame number 94	0.77873	0.62213	0.89726
Frame number 105	0.78627	0.62655	0.90013
Average Value	0.77277	0.638253	0.897382

5. CONCLUSION

This paper conclude a robust and imperceptible video watermarking algorithm using Discrete wavelet transformation in randomly selected frames using secret key. This paper presents a content-based digital video-watermarking scheme, by embedding the watermark in the horizontal coefficient matrices obtained by discrete wavelet transformation to the blue layer of the randomly selected frames as well as using secret key. The Implemented Algorithm is simple blind, more secure and highly robust against various kinds of noise and other manipulations like rotation attacks.

REFERENCES

- A. Sarma and A. Ganguly(July 2012), "An Entropy based Video Watermarking Scheme", International Journal of Computer Applications (0975 – 8887) Vol. 50, No.7.
- [2] G. Bhatnagar and B. Raman(2009), "A new robust reference watermarking scheme based on DWT-SVD", Computer Standards and Interfaces, DOI:10.1016/j.csi.2008.09.031.
- [3] J. Madia et al. (2012), "Video Watermarking using Dynamic Frame Selection Technique", National Conference on Advancement of Technologies – Information Systems & Computer Networks (ISCON – 2012), pp 31-34.
- [4] S. Singh, A. Gawri(Feb. 2013), "A Bit Level and Entropy based Blind Watermarking Scheme for Video Sequence using Random Frame Selection", International Journal of Computer Applications, Vol. 64, No. 12.
- [5] S. Sinha et al. (August 2011), "Digital Video Watermarking using Discrete Wavelet Transform and Principal Component Analysis," International Journal of Wisdom Based Computing, Vol. 1 (2).
- [6] Schyndel Van et al. (November 1994), "A digital watermark", in: Proceedings of the Image Processing, IEEE International Conference, vol.2, pp 86 - 90.
- [7] Yadav Anupma, Yadav Anju (May- 2014), "Comparison of SVD-Watermarking and LSB-Watermarking Techniques", International Journal of Computer Science and Mobile Computing, Vol.3 Issue.5, pp 495-499.