Novel Video Watermarking Technique using Scene Change Detection with DWT

Lesa Ann Thomas
Department of Information Technology
Dr. Mahalingam College of engineering & technology, Pollachi, Tamil Nadu, India

S.Ponni @ Sathya
Assistant Professor
Department of Information Technology
Dr. Mahalingam College of engineering & technology, Pollachi, Tamil Nadu, India

Dr.S.Ramakrishnan
Professor
Department of Information Technology
Dr. Mahalingam College of engineering & technology, Pollachi, Tamil Nadu, India

Abstract- A Video Watermarking using Scene Change Detection algorithm is proposed that identifies an approach for protection of information of a video based on wavelet transformation. First, the scene change analysis is used to detect the motion part of the color video. Any random image is selected which is used in the embedding process. That image is converted into its binary image. In the next step the random keys are generated. Next by using RSA algorithm encryption keys are generated. The values of the random keys denote the location of the keys generated by the RSA algorithm. The RSA algorithm keys are arranged according to the location of the random keys. The newly shuffled values are added with the binary value of the embedding image. This process is the Embedding Process. In extraction step, the original video is not needed and it's the reverse process of embedding. This paper shows a good performance for robustness and also withstands all basic attacks.

Keywords – Red, Green, Blue (RGB), Peak Signal-to-Noise Ratio PSNR, Discrete Wavelet Transform (DWT), pseudorandom number.

I. INTRODUCTION

In today's world the exchange of digital multimedia information has become easy but there are certain disadvantages as well like the illegal copies of the original data. Hence to overcome this disadvantage a technique called digital watermarking has been proposed. Now briefing about digital watermarking, it is the process of hiding the digital information in a carrier signal and it does not have any relationship with the carrier signal. Digital watermarks are mainly used to check the integrity of the carrier signal. Host signal is the one in which the watermark is embedded. A watermarking process is usually divided into two distinct steps (i.e.) embedding and extraction. In the embedding process an algorithm is used to embed the watermark. Then this watermarked video is transmitted to another person. Extraction is an algorithm which is applied to extract the hidden watermark. Video Watermarking is divided into two types: visible and invisible. In visible watermarking the watermark will be visible. But in the invisible watermark the watermark will not be visible. Invisible watermarking [3,4] has three different types they are robust watermarking, fragile watermarking, public and private watermarking. In the robust digital watermarking the embedded image should be obtained exactly as the original image even if there were any modifications. In fragile digital watermarking the extracted image will not be the same as that of the original one due to modifications. Invisible Video Watermarking technique is divided as follows: spatial domain watermarking, frequency domain watermarking and spatial frequency domain [2] Spatial watermarking is applied in the luminance block. In this way, the watermark appears in only one of the color bands and is difficult to view the watermark in a normal way. Watermarking can be applied in the frequency domain [6] by first applying a transform like the Fast Fourier Transform (FFT) and the watermark is applied to low frequencies since high frequencies will be lost during compression. There are three important requirements in video watermarking they are invisibility, robustness and capacity. All these are interlinked to each other. If any one of them is changed it affects the other two.

Furthermore sensitive information [8] like credit cards, transactions and social security numbers should be protected by hackers. For protecting all this encryption method plays a vital role. The main idea of encryption is to transmit the information to the receiver securely without going into the hands of unauthorized users for decryption. There are different algorithms for encryption and decryption they are DES, RSA, HASH, MD-5 etc.
DES is a symmetric algorithm and its key is always represented as 64 bit block. RSA is a public key algorithm the keys are different for encryption and decryption. It uses modular exponential. HASH is used for computing condensed information of a fixed length message. MD-5 is a hashing algorithm.

There are some existent algorithms that were proposed and it is as follows: "Robust Dual Watermarking Algorithm for AVS Video", Yuan-Gen Wang (et al) proposed a robust dual watermarking algorithm for video based on the audio video coding standard (AVS) algorithm. One watermark is embedded in luminance components, whose embedding positions are optimized using the particle swarm optimization (PSO) technique, resisting common signal processing operations such as median filtering, adding noises, and cropping and so on. "A Robust Digital Watermarking Scheme for Video Copyright Protection in the Wavelet Domain", Radu O. Preda (et al) proposed a novel digital watermarking method for video based on multi-resolution wavelet decomposition. The watermark used is a binary image. This watermark is embedded in the wavelet coefficients of the LH, HL and HH sub-bands of the second wavelet decomposition level by quantization. Every bit of the watermark is spread over a number of wavelet coefficients with the use of a key. "Copyright Protection of Color Video Using Digital Watermarking", Majid Masoumi (et al) proposed a robust algorithm based on DWT for video copyright protection. Firstly, the RGB video is converted into YUV color component video, then in order to make the watermark imperceptible, the luminance layer is only used to embed the watermark and the chrominance layer is left unchanged. "Robust Digital Video Watermarking in the Spatial and Wavelet Domain", Radu O vidiu Preda (et al) proposed two methods i.e. Spread-spectrum and quantization based techniques. The watermarks used are binary images, containing the copyright information. The author protects the watermark against singular bit errors with a Hamming error correction code. The spatial domain technique embeds a watermark bit by spreading it in a luminance block but the actual embedding is done using a quantization based approach.

II. PROPOSED ALGORITHM

A. SCENE CHANGE DETECTION

Viptraffic video is considered to be the input video. Scene change analysis is done by using the histogram equalization algorithm which is specified below. Scene change analysis is mainly done to detect the motion parts of the video.

$$if \sum_{i=1}^{h} H\,is\,(G_j\,(i)) > th$$
$$G_j(i) = motion\ frames$$
$$else\ if$$
$$G_j(i) = motionless\ frames$$
$$end\ if$$

Where i is the number of frames, j is the red component frames and th is the threshold. In the above algorithm a histogram is generated for the red components of the input video. Histogram is nothing but a graph and it shows the scene change analysis of all the frames in a video.

B.WAVELET TRANSFORM

There are different reasons for embedding the watermark in the wavelet domain they are as follows: Good space frequency localization, Superior HVS and low cost. The most important step before embedding the watermark is the selection of the wavelet because each wavelet has its own characteristics. Here we choose Haar wavelet.[9]

Let I(m,n) be a digital image and its size should be divisible by 2. Let h(n) and g(n) be the wavelet low pass filter and high pass filter respectively. The image gets decomposed into four coefficients they are LL,HL,LH and HH. The decomposition formula is as follows:

$$\begin{cases} LL(i,j) = \sum_{m,n} h(m-2i)\,h(n-2j)\,I(m,n) \\ LH(i,j) = \sum_{m,n} h(m-2i)\,g(n-2j)\,I(m,n) \\ HL(i,j) = \sum_{m,n} g(m-2i)\,h(n-2j)\,I(m,n) \\ HH(i,j) = \sum_{m,n} g(m-2i)\,g(n-2j)\,I(m,n) \end{cases}$$

Where LL,HL along the horizontal direction, LH along the vertical direction and HH along the diagonal direction.

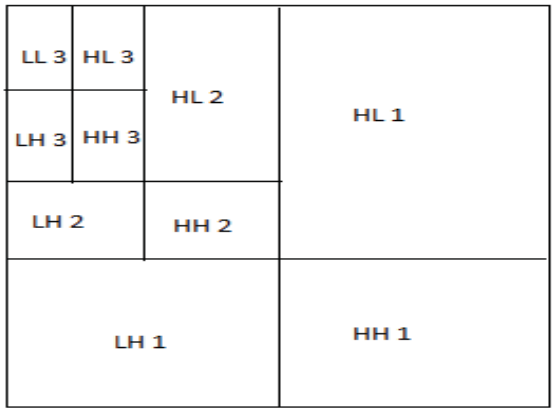


Figure 1. DWT Decomposition model

Here level 1 bands are vulnerable to noise and hence the DWT is applied to LL 2 and those band gets decomposed into four sub bands i.e. LL3, LH3,HL3 and HH3. Since LL3 is low frequency we use the rest of the three sub-bands for embedding process.

Watermark preprocessing- In this process viptraffic video that has 120 frames in total is choosen for watermarking. To perform watermarking cameraman image(256x256) is choosen. The scene change is analysed and the frame with maximum deviation is watermarked with the image.The image is resized according to the the frame, converted into a binary form that contains 0's and 1's and then only it is embedded.

C.EMBEDDING ALGORITHM

1) Once the motion parts of the video is detected, a three dimensional wavelet is applied on the motion part are obtained i.e. LL, LH, HL, HH. LL is not chosen.
2) After applying the three dimensional wavelet, three coefficients are chosen for watermarking since it has a low frequency.
3) Three sets of pseudorandom numbers are generated using the Mersennne-Twister algorithm.
4) After which the embedding algorithm is used using 3D-DWT which is as follows:

$$\begin{aligned} &\text{if } I(i,j) = 0 \text{ then} \\ &C_v(i,j,k) = C_v(i,j,k) + \alpha W_v(i,j,k) \\ &\text{else if} \\ &C_v(i,j,k) = C_v(i,j,k) \\ &\text{end if} \end{aligned}$$

Where α is the intensity factor, I(i,j) is the binary watermark.

5) The input video is selected for the watermarking process. Any image can be selected which is used for embedding in the video.

6) Using Histogram Equalization algorithm the input video is split into RGB channel [7] where only the Red Components are considered. 3DWT is performed for the selected frames.
7) Then the random keys are generated by using Twister algorithm [10].
   Twister Algorithm- The Twister algorithm is used to generate pseudorandom numbers. It provides fast generation of high quality pseudorandom integers.
8) The unique keys are generated by using RSA algorithm.
   RSA Algorithm- RSA algorithm is used to encrypt and decrypt messages. It is an Asymettric cryptographic algorithm. There are two different keys namely Public key and Private key.
9) The random keys are refered as the location for the unique keys.
10) Then the newly replaced values are added with the binary values of the selected image. Finally watermarked video is obtained.
11) Once the embedding process is over, a 3D-IDWT is performed.
12) Fig 2. Explains the embedding process via block diagram.

D.EXTRACTION ALGORITHM

Extraction process is the reverse of embedding i.e.

1) A 3D-DWT is performed on motion part of video.
2) The dimensional coefficients are decomposed by using three level wavelet.
3) Three sets of pseudorandom numbers are generated using Mersenne-Twister algorithm.
4) The watermark is found by calculating the correlation between the extracted coefficients and their pseudorandom numbers.
5) The algorithm for correlation is as follows:

$$if \sum (corr(EC_k(i,j,k), W_k(i,j,k))) > th$$
watermark is detectable
end if

6) In this the newly formed matrix is extracted to its original form by using the key generated in RSA algorithm.
7) Then the matrix is seperaterd from the binary vales of the image. The original video and the watermarked image is obtained.
8) Fig 3. Explains the extaction process via block diagram.

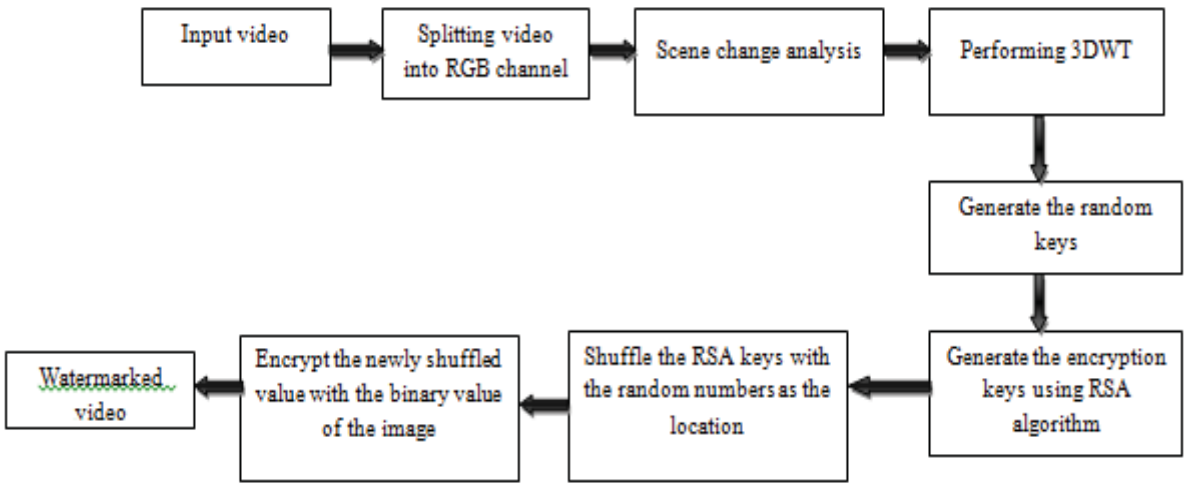


Figure 2. Watermark embedding algorithm Block Diagram

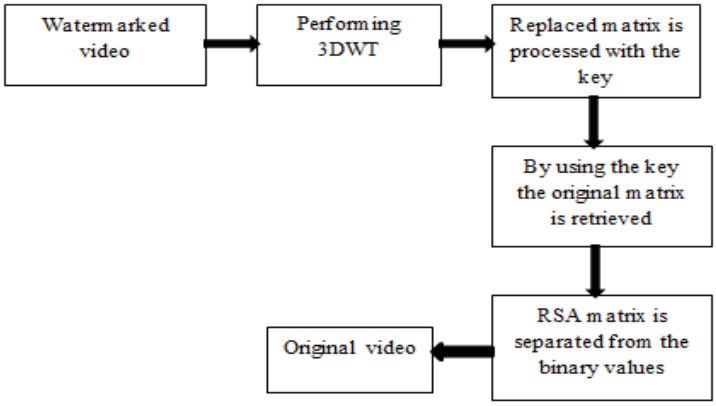


Figure 3. Watermark ectraction algorithm Block Diagram

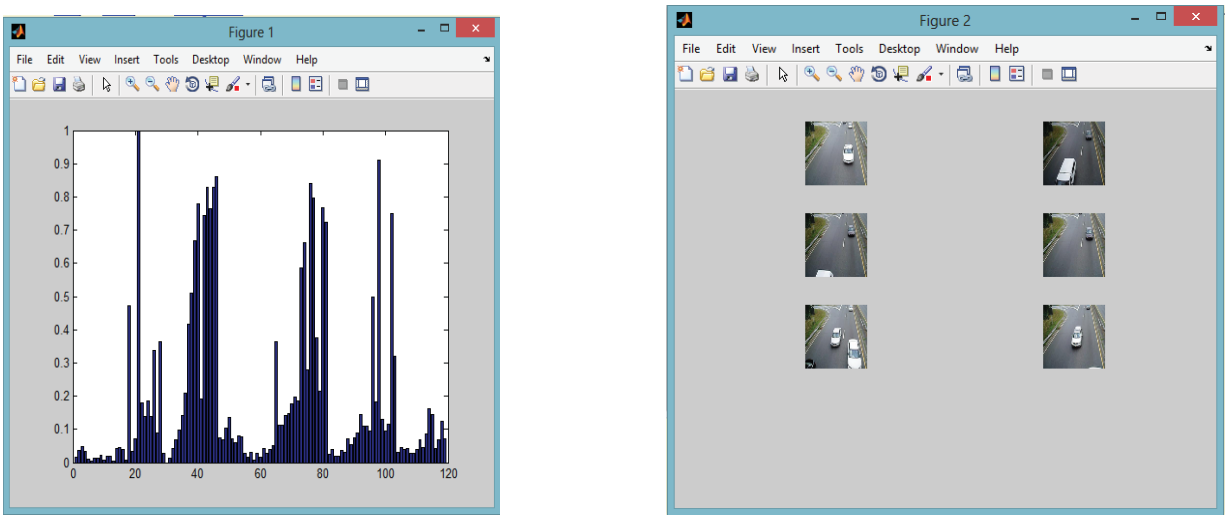
III. RESULT AND DISCUSSION

The watermark image and the input video that is considered is shown in fig.4 and the watermarking process is done on the viptraffic that contains 120 frames of AVI format.

(a) (b)

Figure 4 . (a)Input Video (b)Watermark image

The result for the scene change analysis using histogram equalization algorithm and the frames that the watermark is embedded is shown in fig.5 as well as fig.6 shows the watermarked image that is extracted.



(a) (b)

Figure. 5 (a) Scene change analysis using histogram (b) Watermarked video frames

Figure. 6 extracted image

In order to measure the perceptual quality, the PSNR value is calculated and has the unit dB .

$$PSNR = 20\log_{10}\left(\frac{max_I}{\sqrt{MSE}}\right)$$

Once the PSNR value is calculated the robustness is to be calculated by performing several attacks. The attacks are as follows: Frame Dropping attack is a method in which the frames in the watermarked video are removed and replaced by frames of the non-watermarked video. Frame swapping attack is a method in which the frames are swapped with its next neighbor frame. Addition of noise and Filtering is a method which is used to check the robustness against noise because addition of noise is responsible for degradation and distortion of the video. Hence Gaussian noise with variance 10% and zero mean is applied. Lossy compression is a method used to check the robustness against compression i.e. in order to transmit a video with its large volume is not possible; hence the video is compressed and then transmitted. H.264, MPEG-2 are the different lossy compression techniques. Fig 7. shows the comparisons of PSNR values. When compared to other algorithms the proposed algorithm has minimum noise.

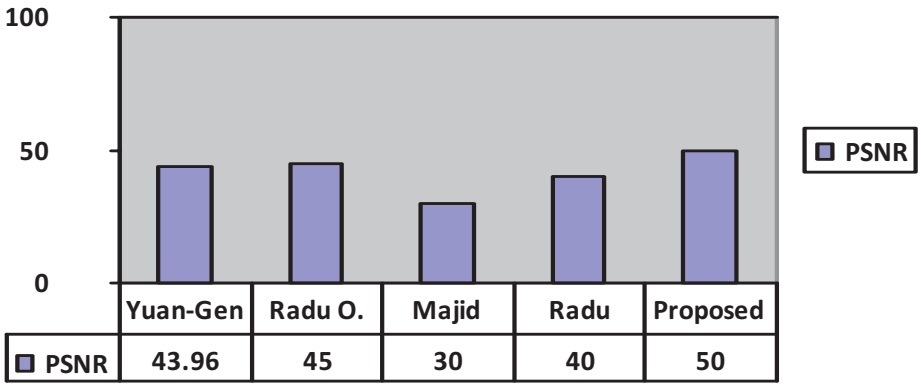


Figure 7. Comparison of PSNR value

IV.CONCLUSION

The proposed method shows good robustness against different attacks like frame dropping attack, frame swapping attack, noise and filtering and lossy compression. The comparison of the proposed algorithm with the existent algorithms shows that the proposed system is more robust than the other algorithms. The perceptual quality is good for this algorithm.

REFERENCES

[1] Majid Masoumi, Shervin Amiri, "A blind scene-based watermarking for video copyright protection", International Journal of Electronics and Communications,2012.

[2] Radu Ovidiu Preda, Cristina Oprea, Ionuţ Pirnog, Lucian Andrei Perişoară,,"Robust Digital Video Watermarking in the Spatial and Wavelet Domain",The Seventh International Conference on Digital Telecommunications, 2012.

[3] M.Mohamed Sathik,S.S Sujatha" A Novel DWT based invisible watermarkingn technique for digital image", Internation Arab Journal of e-Technology,Vol.2, No. 3,2012.

[4] Pallavi Patil, D.S.Bormane," DWT based invisible watermarking for digital images", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-2, Issue-4, April 2013.

[5] Radu O. Preda, Dragos N. Vizireanu," A robust digital watermarking scheme for video copyright protection in the wavelet domain", Measurement 43 (2010) 1720–1726

[6] Nisreen I. Yassin, Nancy M. Salem, and Mohamed I. El Adawy," Block Based Video Watermarking Scheme Using Wavelet Transform and Principle Component Analysis", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 3, January 2012

[7] Majid Masoumi, Shervin Amiri," Copyright Protection of Color Video UsingDigital Watermarking," IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 4, No 2, July 2012.

[8] Hamid Shojanazeri1, Wan Azizun Wan Adnan2, Sharifah Mumtadzah Syed Ahmad," Video Watermarking Techniques for Copyrightprotection and Content Authentication," International Journal of Computer Information Systems and Industrial Management Applications volume 5 (2013) pp. 652–660.

[9] Liu JF, Huang DR, Hu JQ "The orthogonal wavelet bases for digital watermarking "J Electron Inf Technol 2003;25:453–9.

[10] Matsumoto M, Nishimura T. Mersenne Twister, "A 623-dimensionally equidistributed uniform pseudorandom number generator", ACM Trans Model Comput Simul 1998;8:3–30

[11] Yuan-GenWang, Zhe-MingLu, LiangFan a, YunZheng," Robust dual watermarking algorithm for AVSvideo", Signal Processing: Image Communication 24 (2009)333–344