SOCIETY FOR SCIENCE AND EDUCATION
UNITED KINGDOM

AIVP ADVANCES IN
IMAGE AND VIDEO PROCESSING

VOLUME 4, ISSUE 6
ISSN 2054-7412

Frequency and Boolean Based Secret Shared Watermarking for Authentication of Video Data

[1]S. Bhargavi Latha, [2]D.Venkat Reddy and [3]N.Krishna Chythanya
[1,3]*Compter Science and Engineering, GRIET, Hyderabad, India;*
[2] *Electronics and Communication Engineering, MGIT Hyderabad ,India,;*
s.bhargavilatha@gmail.com;dasari_reddy@yahoo.com, kcn_be@rediffmail.com

ABSTRACT

Video watermarking refers to the process of embedding authentic patenting information in to bit streams of videos. The authentication of the digital data has become the need of the hour in this digital era. This paper emphasizes the combined use of frequency domain and Boolean based secret sharing scheme for generating an authentication using watermarked video frames.

Keywords: Video watermarking; frequency domain; XOR; scrambling; piracy attacks.

1 Introduction

In the era of ubiquitous computing, the world turned in to a global village and every need of the day is just at a finger touch away. Internet is playing significant role with large volumes of data being maintained in digital form. The authentication of the digital data has become the need of the hour in this digital era. Let it be medical field , general communication, Banking/Financial sector or in general in any digitized data management systems, the impact of significant and rapid growth of ICT is very high, this leading to the vast growth of digital media access and modification or alterations over group of connected systems. And hence protecting digital information with proper copyright has become inevitable**.**

In order to reap the benefits of easy distribution, saving and first of all efficient creation of digital multimedia, A digital watermarking technique has become an impending feature for Authentication. And such a technique needs to be transparent, should also resist the attacks which may dispose the watermark or exchange it with a new watermark. In other words strength of withstanding the common signal processing operations such as rotations, compressions and filtering etc should be very high.

Among the techniques of authentication for digital media in the form of image, the relatively new technology was required to solve the illegitimate manipulation and sharing problem of digital videos and this lead to the beacon of research in the area of video watermarking. Frame averaging, piracy attacks etc are general practice of attacks on videodata owing to inherent redundancies among frames and because of large quantity of information through videos.

Video watermarking refers to the process of embedding authentic patenting information in to bit streams of videos**.**

The embedding of author's ADHAAR card number, or logo of his/her organization or images/text with some unique identification belonging to the author and so on can be done through watermarking

DOI: 10.14738/aivp.46.2534
Publication Date: 23rd January, 2016
URL: http://dx.doi.org/10.14738/aivp.46.2534

using certain algorithms. The exponential growth of cyber crimes over the past decade is an easy measure to understand the demand for a legitimate authentication requirement of digital video data that is being shared through the network. It should also be noted that a video is an ordered set of image frames but also has an extra dimension in "time" which provides a remarkable adjustability and complexity for solution space as compared to that of Image watermarking.

Digital watermarking is more than just a decade old proposal to protect copyright information for multimedia documents. The videos generated could be of Internet uploaded, videos over wireless, or recorded over video phones or might have resulted because of some video conferencing event. But illegal/ illegitimate copying of or sharing of such video need to be curbed.

This paper emphasizes the combined use of frequency domain and Boolean based secret sharing scheme for generating an authentication using watermarked video frames.

The remaining paper is organized as section 2 gives an overview of related research work done on the bases of image as well as video watermarking, Section 3 presents the algorithm used by the authors, Section 4 gives the experimental results as carried out by the authors, Section 5 concludes the paper with section 6 giving information of required references for further study.

2 Related Work

Based on whether spatial pixel values are used for embedding and detection or alteration of spatial pixel values happened as per a pre-determined transform function, the approaches of video watermarking are categorized into spatial domain watermarking or transform domain watermarking respectively. Though easy to implement, spatial domain techniques are yet prone to attacks such as compression of videos. The disposing of watermarking in the spatial domain of a frame of any video makes transform domain technique more robust as compared to spatial domain technique.

The image watermarking algorithms makes use of image transforms such as Discrete Wavelet Transform, Discrete contourlet transform , or Discrete Cosine transform, of which the contourlet transform is capable of capturing the bi directional edges of the image at different scale. The different techniques opted by many researchers on video watermarking can be simply put in the following diagram Fig1.

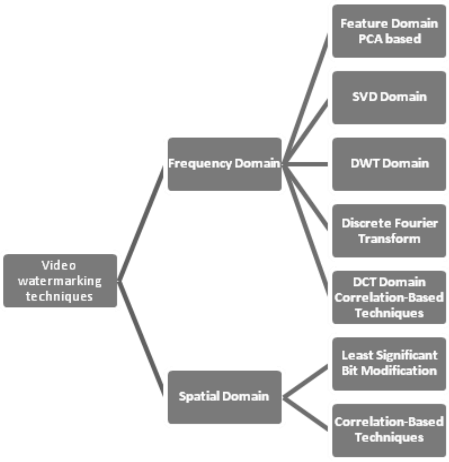

Video watermarking techniques
Frequency Domain
Spatial Domain
Feature Domain PCA based
SVD Domain
DWT Domain
Discrete Fourier Transform
DCT Domain Correlation-Based Techniques
Least Significant Bit Modification
Correlation-Based Techniques

Figure 1: Techniques of video watermarking.

Principle Component Analysis applied for blocks generated using DWT and watermark is embedded in to the maximum coefficient of principle component analysis blocks of two bands in the work carried out by Nisren & Yassin[10].The work successfully shown robustness against many attacks such as i.Gaussian noise addition, ii.Gamma correction, iii.JPEG coding etc.

Prachi V, etal.. developed a robust low power scheme based on FPGA implementing invisible insertion of water marking and the experiment was carried out on VERTEX-6 FPGA using Very High Speed Integrated Circuit Hardware Description Language.[11]

Research shows there are many piracy attacks possible on video data such as shown in the figure Fig2.

In one of the researches DWT method was implemented in which using shot segmentation technique initially the input video clip is partitioned in to non-overlapping segments known as shots.

Based on the relative importance played by each bit of the image, the image is embedded in to each segment of video. [12] proved that such process provides better results and high accuracy. [13] have developed a hybrid optimization technique by inserting unseen and vigorous watermark information in to the video stream. In [4] an audio water mark was embedded in to the video to provide authentication for the creator and the work was based on CWT& CS algorithm.

Where as LamRajab et al in [5] have worked on SVD transform based video watermarking. The SVD concept was so that each singular value indicates the luminance of an image layer which the corresponding pair of singular vectors specifies the geometry of the image layer and the frame image was further divided in to three matrices decomposed from one matrix.

These days a new proposal is being considered in which Researchers use watermarking combined with secret sharing. Two different shares of watermark image are created and these both shares need to be combined to get back the watermark image. Off these two shares one share is kept undisclosed and other share is used in embedding to give watermarked image. Young Chang worked on inserting watermark image in spatial domain and is called as asymmetric watermarking procedure. But Cropping, filtration etc attacks can make it vulnerable. Usage of JND to calculate scaling factor for embedding in the frequency domain was carried out by Shang-Lin Hsieh [14] but this method requires use of code book and also results in pixel expansion of images shared apart from low accuracy. Boolean operation based secret sharing was suggested as a solution for the above problem by the researchers.

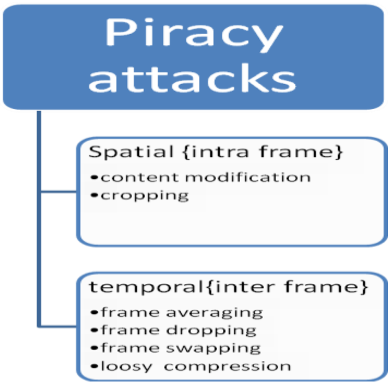


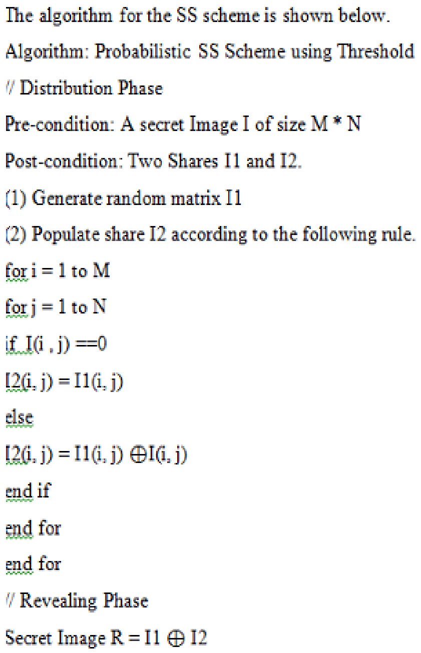
Figure 2:Piracy attacks on video data

3 Proposed Idea

The process of embedding includes converting the host video clip in to number of video frames and a binary image is considered for watermarking. The sub band coefficients of the image are produced by applying DWT on Red channel of the watermark image. Water mark bits are embedded on the calculated singular values. Initially the water mark is scrambled then SS scheme is applied to generate shares, of which one is used in embedding and the other one in retrieval process.

The authors follow the procedure shown in [6] and following algorithm is used to implement secret sharing scheme using threshold.

Secret Sharing SCHEME USING THRESHOLD



```
The algorithm for the SS scheme is shown below.
Algorithm: Probabilistic SS Scheme using Threshold
// Distribution Phase
Pre-condition: A secret Image I of size M * N
Post-condition: Two Shares I1 and I2.
(1) Generate random matrix I1
(2) Populate share I2 according to the following rule.
for i = 1 to M
    for j = 1 to N
        if I(i , j) ==0
            I2(i, j) = I1(i, j)
        else
            I2(i, j) = I1(i, j) ⊕I(i, j)
        end if
    end for
end for
// Revealing Phase
Secret Image R = I1 ⊕ I2
```

The detailed algorithm for embedding and extracting watermark image is as follows:-

A. Watermark embedding process:

The following are the details of the algorithm

Algorithm: steps to carry out for Embedding Watermark.

Input : Host Video, Watermark (Binary) image WM(K×L).

Output : Watermarked Video(M×N).

Step1: The host video is used to extract video frames (VF1, VF2…VFn) of dimensions M×N, which need to be authenticated.

Step2: Consider any binary image of dimension K×L to be used for watermarking, call it as WM.

Step3: Extract the RED channel (R) from VFi.

Step4: Extract LL sub-band by applying DWT on R channel.

Step 5: Assortment of Watermark Image WM is done to get scrambled image which reduces Geometric attacks on the WM.

Step6: Using (2,2) SS scheme as explained later in this paper,Two shares of WM S1, S2 having same size are generated. Of these two shares S1 is undisclosed and S2 is considered for embedding.

Step7: A (K*L) size 1D matrix is generated by reshaping S2 and then the bipolar form of that matrix is considered for next steps.

Step8:16 ×16 non overlapping blocks of LL Band is to be obtained.

Step9: For i=1 to M/16×N/16, do Step9.1 to Step 9.3

```
        Step 9.1: U, S, and V values are obtained by applying SVD.
        Step 9.2:S1= S1+beta*watermark bit   formula is used for watermark embedding into singular value.
        Where beta is the embedding factor
        Step9.3: Inverse SVD is applied by considering the modified S values.Step10: Inverse DWT is applied.
Step11: The watermarked video frame is finally obtained by concatenating G and B channel with modified R channel.
```

B: Extraction of Watermark (WM) Process

The following are the details of the algorithm

Algorithm: steps to carry out for Embedding Watermark.

Input: Video frame extracted from the watermarked Video WMVF (M×N), Host video frameVF(M×N), S1 share(K×L).

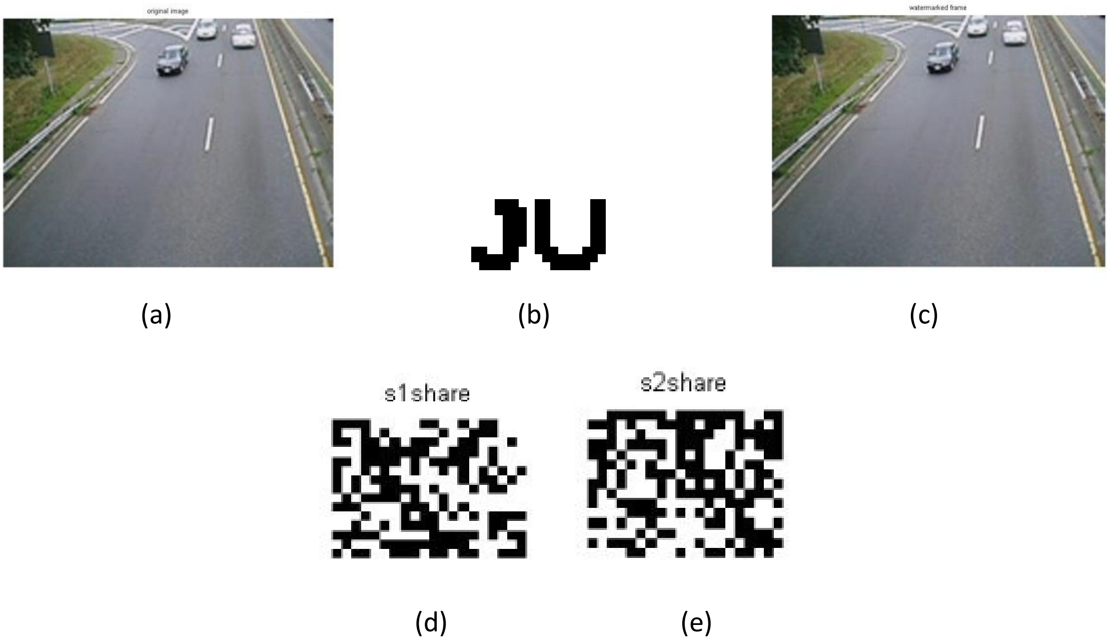
Output: Watermark image WM (K×L).

```
Step1: Watermarked video frame WMVF of size M×N.
Step2: LL Sub-Band isacquired  applying DWT to  R channel.
Step3: Divide the LL Band into16 ×16 non-overlapping blocks
Step4: For i=1 to M/16×N/16, do Step4.1 to Step 4.2
  Step 4.1:Oobtain UW, SW, and VW values by applying SVD.
  Step 4.2: Singular values are used to extract the share bits by using the following formula
        (SW1-S1) > 0 then extracted share bit=1
      Else 0
Step 5: Reshape the watermark into the size of K×L.
Step 6: S1 share and extracted share are XORed to get scrambled watermark.
Step 7: The original watermark can be obtained by descrambling the output of step6.
```

4 Experimental Results

Initially, MATLAB based implementation was done to evaluate robustness of the idea. A watermark image of size 15x20 generating similar size secret shares watermarks is used for simulation purpose. Video in avi format of size 640x480(car.avi)with 200 frames is considered. In order to avoid Burst errors, row-column transformation method is used to scramble the secret share image. DWT and SVD techniques are used for embedding the shared image. DWT in watermarking is already a proven robust method as compared to DCT/DFT hence it is opted for this experiment.

The following figure shows the one example frame of video, watermark, generated secret shares and watermarked frame.



(a) (b) (c)

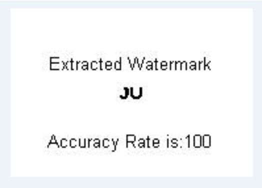
(d) (e)

Fig 3: a) Video Frame b) watermark c) watermarked Video frame d) S1 share e) S2 share

To measure the visual quality Accuracy rate (AR) is used which is given in the following equation.

$$AR=CP/NP \qquad (1)$$

Where NP is How many number of pixels are there in the Original image, and CP is the number of pixels that are matched in both the images. The following figure 4 shows the extracted watermark along with AR when no attack is applied to the frame of the avi video.

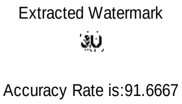

Extracted Watermark

JU

Accuracy Rate is:100

Figure 4: Extracted watermark with AR and no attack.

The following figure 5 shows the retrieved water mark after applying salt & pepper noise with the noise density of 0.04 in the watermarked image

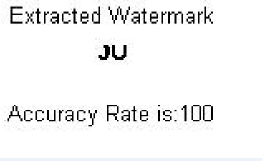

Extracted Watermark

JU

Accuracy Rate is:91.6667

Figure 5: Retrieved watermark image after salt& pepper noise

The following figure 6 shows the extracted watermark after applying resize attack with resize factor of 3.


Extracted Watermark

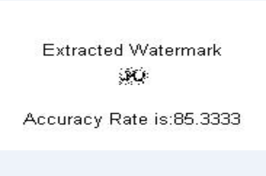
JU

Accuracy Rate is:100

Figure 6: Extracted after Resize attack

Copyright © Society for Science and Education United Kingdom

The following figure 7 shows the extracted watermark after applying Gaussian noise to the watermarked image with sigma value of 1.

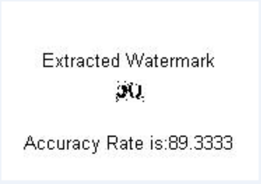


Extracted Watermark

Accuracy Rate is:85.3333

Figure 7 Extracted after applying Gaussian noise

The following figure 8 shows the watermark after applying cropping attack on the video watermarked image by 30 by 30.

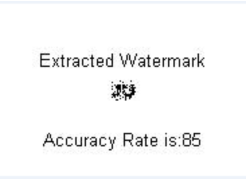


Extracted Watermark

Accuracy Rate is:89.3333

Figure 8 Extracted after applying cropping attack.

The figure 8 above shows the watermark after applying compression with quality factor of 80

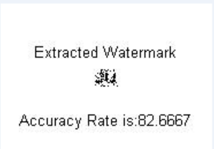


Extracted Watermark

Accuracy Rate is:85

Figure 9 Extracted after compression.

The following figure10 shows the watermark after applying sharpening attack.

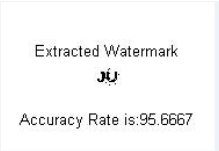


Extracted Watermark

Accuracy Rate is:82.6667

Figure 10 Extracted after sharpening attack

The following figure11 shows the watermark after applying motion blur attack



Extracted Watermark

Accuracy Rate is:95.6667

Figure 11 Extracted after motion blur attack.

5 Conclusion

In this work , a novel approach based on frequency domain and Boolean based secret sharing scheme for generating an authentication using watermarked video frames is successfully implemented and also it is observed that the procedure holds good with respect to all the attacks possible on video data such as salt&pepper noise, Resize attack ,Gaussian noise, cropping attack compression , sharpening attack and also motion blur attackThe experiments are performed as follows:

REFERENCES

[1]. Hybrid Contourlet-DCT Based Robust Image Watermarking Technique Applied to Medical Data Management(Watermarking, Stegnography and Biometrics), http://what-when-how.com/pattern recognition-and-machine-intelligence. Sept 2016.

[2]. B.Chnadramohan,S.Srinivas kumar, A Robust Image Watermarking Scheme using Singular Value Decomposition—Journal of Multimedia,Vol 3, No.1, May 2008,Pg-7-15,Academy publishers.

[3]. Ibrahim A.El rube et al ,Contourlet versus Wavelet ransform for a Robust Digital Image Watermarking Technique, http://waset.org/journal/computer, vol 3 No:12,2009 pg 2303-2307.

[4]. M. Sundararajan, G. Yamuna, CWT and CS Algorithm Based Video Watermarking Using Audio Watermark, Procedia Computer Science, Volume 87, 2016, Pages 93–98 Fourth International Conference on Recent Trends in Computer Science & Engineering (ICRTCSE 2016) pg 93-98.

[5]. Lama Rajab, Tahani Al-Khatib et al Video Watermarking Algorithms Using SVD Transform, European Journal of Scientific Research.ISSN 1450-216X Vol.30 No.3 (2009), pp.389-401 www.eurojournals.com/ejsr.htm

[6]. Abhishek Mishra and Ashutosh Gupta, Secret Sharing Schemes using Thresholding, International Journal of Computer Science and Information Technology & Security (IJCSITS), ISSN: 2249-9555,Vol.6, No1, Jan-Feb 2016

[7]. Chen TH, Tsao KH, Threshold visual secret sharing by random grids. Journal of Systems and Software 2011; 84:1197–1208

[8]. Sachin Kumar and Rajendra K. Sharma, Threshold visual secret sharing based on Boolean operations", SECURITY AND COMMUNICATION NETWORKS Security Comm. Networks 2014; Vol7,p.p.653–664.

[9]. Hamid Shojanazeri,Wan Azizun Wan Adnan et al,Video Watermarking Techniques for Copyright protection and Content Authentication,International Journal of Computer Information Systems and Industrial Management Applications, ISSN 2150-7988 Volume 5 (2013) pp. 652–660.

[10]. Nisreen I. Yassin, Nancy M. Salem, 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 ISSN (Online): 1694-0814

[11]. Prachi V. Powar(2013). Implementation of digital video watermarking scheme based on fpga,International Journal of Electrical, Electronics and Computer Systems, vol.1 , pp. 99 -104 .

[12]. M.Sundarajan,G.Yaamuna, A wavelet based scheme for video watermarking, International reiew on computers and software 2013, pg 1023-1032.

[13]. Puja Agarwal,Khurshid.A.,DWT and GA-PSO Base Noval Watermarking for Video Using Audio Watermark for videos using Audio watermarking- Advances in swam intelligence, ICSI,Hefie,China p212-220.

[14]. Shang-Lin Hsieh, I-Ju Tsai, Bin-Yuan Huang, and Jh-Jie Jian, Protecting Copyrights of Color Images using a Watermarking Scheme Based on Secret Sharing and Wavelet Transform, Journal of Multimedia, vol. 3, No. 4, 2008, pp. 42-49.