Genuine Video Steganography Validation Using Combined Comparable Wavelet Transforms

G S Siva Kumar[1], M Ravi Kumar[2], Associate Professor[1], PG scholar[2]
ECE Department, Pragati Engineering College, E.G. Dist, A.P, India[1&2].
[1]skgompa@yahoo.com,[2]ravikumarmanchim@gmail.com

Abstract— **With the raising robustness in the technology any statistics can be extrapolated where they show disaster. One such affliction of the enormously developed communication system is hacking. This paper intends to propose the possible methods for the Genuine video copyright validation using Steganography, invisible watermarking technique and also comparative analysis between different wavelet transforms. The watermarked (N-1) th frame is segregated with compressed sensing algorithm from the rest of the video and the certification of pre-generated robust authentication is carried on in to which watermarking bits are engraved with the low frequency Daubechies transform. Simulation results show that the algorithm has better detection ability and detection accuracy than invertible semi-fragile watermarking algorithm distinguishing compression from malicious manipulation of the algorithm. Robust watermarks are detectable even after some image processing operations has been performed on the watermarked image such as image scaling, bending, and cropping, and so on which is not shown in the remaining two techniques of fragile and semi fragile watermarking.**

Keywords— **Daubechies transform; invisible watermarking; robust watermarking; fragile watermarking; semi fragile watermark; Steganography; compressed sensing; copyright validation**

I. INTRODUCTION

With the raising of multimedia soft wares for video and images tampering of audio and video has risen immensely. Therefore video copyright validation technology gained substantial importance both commercially as well as technically. This paper introduces a method for obtaining the location identity of the segment where our transmitting video has been hacked. This method involves scribing of concealed messages or images commonly known as watermarking on one of the isolated frames of the video. For the sake of tamper detection the video is deframed in to N frames using Daubechies transform and the (N-1) th frame is our work site. The watermark signature bits are appended in to the components of the transform depending upon our requirement. Then these frames are then again framed to form the to be transmitted video. The watermarked bits contain the information like the geographical identities of the place to which it is transmitted so that the tracing of location is at our hands. The Daubechies formulation is based on the use of recurrence relations to generate progressively finer discrete samplings of an implicit mother wavelet function; each resolution is twice that of the previous scale.

This paper mainly stresses on the importance of robust watermarking which is inevitable for achieving protection against malicious manipulation as well as benign manipulation techniques like video tampering, cropping, scaling etc., where the semi fragile watermarking is resilient to only benign transformations.

This paper is organized as the following sections: section II introduces the complex technique of video de-framing, section III introduces the algorithm of the watermarking technique utilized and section III explains and presents a comparative analysis of the wavelet transforms and the following sections constitute the valedictory part.

II.VIDEO DEFRAMING

For the purpose of securing user’s or receiving area’s identity it is not necessary for the entire video to be watermarked. It is enough if one of the frames of the video is marked. For the process the procedure deployed by us starts with the complex algorithm of Deframing of the video. It is the procedure of dividing the transmitting video into N (the number of frames) frames. Its value depends upon the type of quality we are going to expect from the video. There are a number of methods for the extraction process. Few such are mentioned here within: Vermaak et al difference threshold methods, Girgensohn’s cluster representation method, Lee’s energy minimization method, Lin et al key frame extraction method based on multi scale phase based local features corner detector, Yang et al statistical model. The main drawback of these methods is that the number of key frames cannot determine automatically to capture adequately the major video content.

The above problem can be solved by using a key frame extraction method based on information bottle neck method. We use improved Bayesian Information Criterion to determine the number of information bottle neck method and then extract using the improved cluster method.

1) *Information bottle neck algorithm:*

The key frame extraction is based on information theoretic principle, the information bottleneck method (IB) recently produced by Trishby et al. the IB principle can be motivated from Shannon's rate distortion theory. The IB principle states that among all the possible clusters of the set into a fixed number of clusters.

According to the IB principle assume that there is object space X and feature space Y .We seek a clustering x such that, given a constraint on the clustering quality *I(X; x)* the information loss *I(X, Y) – I(x, Y)* is minimized.

II. WATERMARKING ALGORITHM

The watermarking technique employs the steganographic techniques of concealing the identity recognizing object in one of the frames of the video so that it becomes a means for identifying the area where our was hacked by the external agencies. The algorithm of the watermarking concept can be given as here under:

- Extract loaded color video into frames.
- Apply block matching motion estimation techniques on the subsequent frames.
- Select only those frames that have sufficient number of motion blocks which is compatible with the watermark size.
- From the selected frames use a given threshold to select the best blocks during the matching process.
- Perform the wavelet transformation on the selected best blocks.
- Extract the embedded watermark.
- Apply some attacks on the watermarked frames in the video.
- Evaluate the conducted results using PSNR for embedding and similarity for extracting process before and after attacks.
- Embed a random Gaussian distribution as a proposed watermark into the selected blocks (Apply only to the HL and LH wavelet bands).

In the next section, we describe an existing technique for spatial video watermarking and adapt this algorithm to design a frequency based video watermarking.

IV. WAVELET TRANSFORMS

Wavelet transforming refers to the transforming of our video from time domain to the spatial domain. This is because certain operations we perform in spatial domain have significant advantages over that in the time domain or spatial domain or frequency domain. Operations like direct manipulation of the pixels, enhancement of some pixels etc., are possible in spatial domain only.

The process followed here is explained here through a flow diagram.

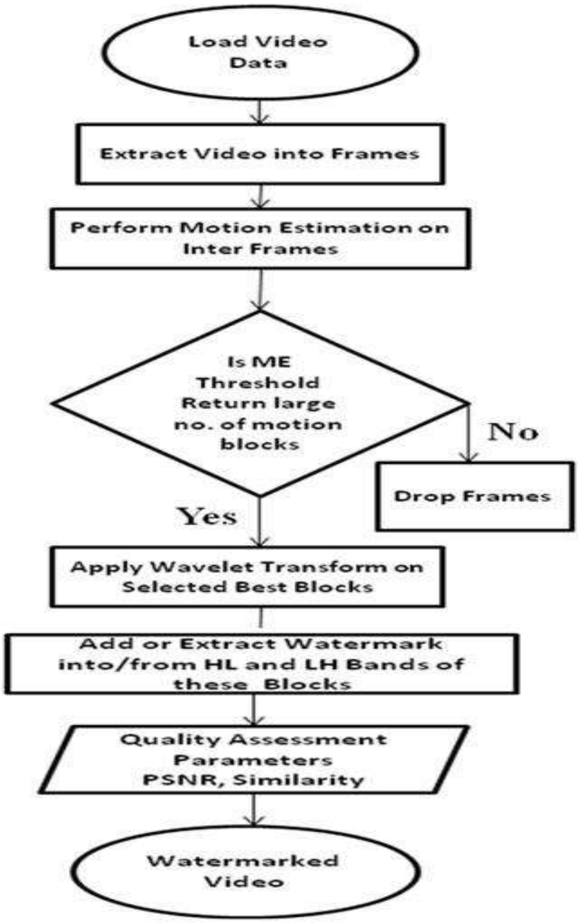
Load Video Data
Extract Video into Frames
Perform Motion Estimation on Inter Frames
Is ME Threshold Return large no. of motion blocks
No
Drop Frames
Yes
Apply Wavelet Transform on Selected Best Blocks
Add or Extract Watermark into/from HL and LH Bands of these Blocks
Quality Assessment Parameters PSNR, Similarity
Watermarked Video

Fig. 1 Video watermarking flow chart

The below provides the procedure for inverse watermarki -ng:

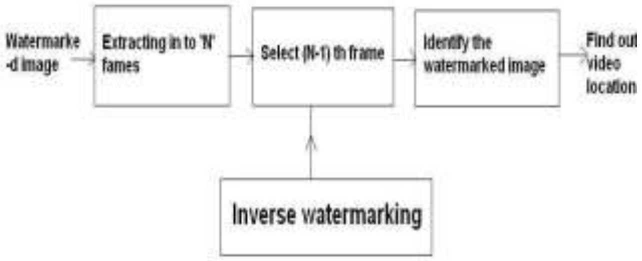

Fig 2. Inverse watermarking flow chart

Common applications of wavelet transforms include:

- Speech and audio processing
- Image and video processing
- Biomedical imaging
- 1D and 2D applications in communications and geophysics.

The type of transformation we make use is the Discrete wavelet transform

Discrete Wavelet transform (DWT) is a mathematical tool for hierarchically decomposing an image. It is useful for processing of non-stationary signals. The transform is based on small waves, called wavelets, of varying frequency and limited duration. Wavelet transform provides both frequency and spatial description of an image. Unlike conventional Fourier transform, temporal information is retained in this transformation process. Wavelets are created by translations and dilations of a fixed function called mother wavelet.

Some commonly used types of Discrete Wavelet Transforms are

- Haar Wavelets
- Daubechies Transform
- BiOrthogonal Transform
- Dual Tree Complex Wave Transform etc.,

1) *Daubechies Transform*

The most commonly used set of discrete wavelet transforms was formulated by the Belgian mathematician Ingrid Daubechies in 1988. This formulation is based on the use of recurrence relations to generate progressively finer discrete samplings of an implicit mother wavelet function; each resolution is twice that of the previous scale. In her seminal paper, Daubechies derives a family of wavelets, the first of which is the Haar wavelet. Interest in this field has exploded since then, and many variations of Daubechies original wavelets were developed.

In general the Daubechies wavelets are chosen to have the highest number *A* of vanishing moments, (this does not imply the best smoothness) for given support width *N=2A*. There are two naming schemes in use, D*N* using the length or number of taps, and db*A* referring to the number of vanishing moments. So D4 and db2 are the same wavelet transform.

Among the 2^{A-1} possible solutions of the algebraic equations for the moment and orthogonality conditions, the one is chosen whose scaling filter has extremal phase. The wavelet transform is also easy to put into practice using the fast wavelet transform. Daubechies wavelets are widely used in solving a broad range of problems, e.g. self-similarity properties of a signal or fractal problems, signal discontinuities, etc.

The Daubechies wavelets are not defined in terms of the resulting scaling and wavelet functions; in fact, they are not possible to write down in closed form. The graphs below are generated using the cascade algorithm, a numeric technique consisting of simply inverse-transforming [1 0 0 0 0 ..] an appropriate number of times.

2) *Bi Orthogonal Transform*

The scaling equations on the scaling functions and wavelets show that the decomposition and reconstruction of a signal from a resolution to the next one is implemented by perfect reconstruction filter banks.

$$a1\ [n] = a0 * h1\ [2n]$$

And

$$d1\ [n] = a0 * g1\ [2n].$$

With

$$h1\ [n] = h\ [-n] \text{ and}$$

$$g1\ [n] = g\ [-n].$$

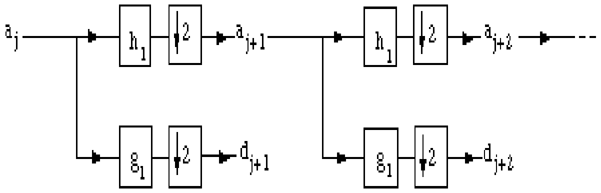

Fig.3 Bio Orthogonal Wavelet Decomposition

In practice this recursion is initialized by considering that the discrete signal samples are some fine resolution coefficients.

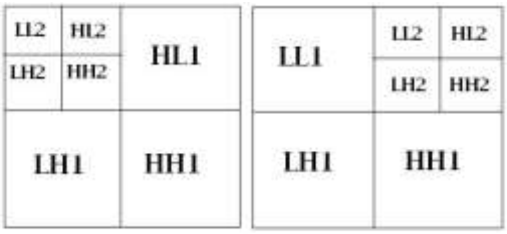

Fig.4 Sub-band Representation

In second level decomposition L represents the approximation sub-band, HL represents the horizontal sub-band, LH represents the vertical, and HH represents diagonal sub-band.

V.EXAMPLES

After the motion estimation is performed on the successive frames in a tested video, the best matching blocks are found. According to the size of the watermark (32*32), a specific number of blocks are needed. In the proposed scheme the nearest blocks from the center are chosen as a criterion

(a) (b)

(c)

Fig.5.*(a) Original Image, (b)* watermarked image after Daubechies wavelet transform method and (c) Dewatermarked image Daubechies wavelet transform method

(a) (b)

(c)

Fig.6.*(a) Original Image, (b)* watermarked image after Biorhogonal wavelet transform method and (c) Dewatermarked image Biorthogonal wavelet transform method

1) *Performance criteria:*

It represents the systems efficiency to effectively generate the video after obtaining the hidden water mark using robust techniques.

The criteria used for representing the efficiency are PSNR and tamper detection rate

As a measure of distortions introduced by watermarking process, the visual quality of the watermarked data is required to be as high as possible. Visual quality means that the degradation of the data due to the watermarking operation should be imperceptible. The Peak Signal to Noise Ratio PSNR is used as visual quality measurement.

$$\text{PSNR(dB)} = 10\log_{10}\left(\frac{m^2 \max(I(x,y))^2}{\sum (I(x,y) - I_w(x,y))^2}\right)$$

Where

I: the original frame data, *Iw*: the watermarked frame data
W: the watermark data , α :the scaling factor,
x, y: 0…...m-1 where m is the block size.

The calculation formula of the tamper detection rate is shown as the formula (8).

$$A=R\,/\,N$$

Here, N is the number of detecting tampered block; A is the total number of tampered block

VI.RESULT ANALYSIS

The adopted test strategy was based on determining the effects of the involved parameters on the performance parameters (Similarity and PSNR) as follows:

1. Number of wavelet pass (taken as constant = 2).
2. Block size (taken as constant = 8).
3. Watermark size (taken as constant = 512 or 1024 bytes)
4. Threshold of motion estimation to return more than 128 motion blocks according to the watermark size (taken as constant = 4).

5. Scaling factor α has not a direct effect in frequency domain due to the small values of wavelet coefficients (taken as constant = 0.1).
6. If any frame contains less than 128 motion blocks, they consider as a dropped frames.
7. Similarity between original and extracted watermark before and after attacks (taken as variable).
8. PSNR between original and extracted watermark before and after attacks (taken as variable).

TABLE 1
PSNR and Temper detection rate for different wavelet transforms

Wavelet transform method	**PSNR value (db)**	**Tamper detection Rate**
Daubechies method	34.86	0.933
Bi-orthogonal method	33.53	0.925

VII.CONCLUSION

This paper presents a development for the applications of water marking through which the unique author's identity is available and the chance of obtaining the place of hacking is able to be known by the embedded watermark in to the selected frame which is (N-1) th frame in our paper.

REFERENCES

[1] J. Lee et al, A survey of watermarking techniques applied to multimedia, IEEE International Symposium on Industrial Electronics, Vol. 1, pp. 272-277, 2001.

[2] Frank, Watermarking of Uncompressed and Compressed Video, Vol. 63, No. 3, pp. 283-301, 1998.

[3] Cox et al, Digital watermarking: principles and practice, Morgan Kaufmann, 2002.

[4] Aree and A. Jamal, Efficient Video Watermarking using Motion Estimation Approach, Proceedings of the 8th IEEE/ACIS International Conference on Computer and Information Science, pp. 593-599, Shanghai, China, 2009.

[5] R. Lancini et al, A robust video watermarking technique in the spatial domain, 4th EURASIP-IEEE Region 8 International Symposium on VIPromCom, pp.251-256, 2002.

[6] P. Meerwald et al, Attack on Watermarking Method Based on Significant Difference of Wavelet Coefficient Quantization, IEEE Multimedia, Vol. 11, No. 5, pp. 1037-1041, 2009.

[7] X. Kang et al, A DWT-DFT Composite Watermarking Scheme Robust to both Affine Transform and JPEG Compression. IEEE in CirSys Video, Vol. 13, No. 8, pp. 776-786, 2003.

[8] E. George and A. Aree, Fast Predictive Coding Method Based on an Enhanced Blocks Motion Estimation, Proceeding in IPCV'08, Nevada, USA, 2008.

[9] M. Rehan et al, A New Motion-Estimation Technique for Efficient Video Compression, IEEE Pacific Rim Conference, No. 1, pp. 326-330, 1997.

[10] Cheng et al, Popular Biorthogonal Wavelet Filters via a Lifting Scheme and its Application in Image Compression, IEEE Proc.-Vis. Image Signal Process., Vol. 150, No. 4, 2003.

[11] Tahani Al-Khatib et al, A Robust Video Watermarking Algorithm, Journal of Computer Science, Nov, 2008, pp. 910-915.

[12] Cox, A Secure Robust Watermark for Multimedia, Information Hiding in Computer Science, Vol. 1174, pp. 183-206, 1996. Cheng et al, Popular Biorthogonal Wavelet Filters via a Lifting Scheme and its Application in Image Compression, IEEE Proc.-Vis. Image Signal Process., Vol. 150, No. 4, 2003

.