NOVATEUR PUBLICATIONS
International Journal Of Research Publications In Engineering And Technology [IJRPET]
ISSN: 2454-7875
VOLUME 2, ISSUE 7, July -2016

VIDEO ENCODING WITH AUTHENTICATION USING MULTIWAVELET TRANSFORM

Pritam R. Durgule
M.E. Scholar, T.K.I.E.T. Warananagar
Prof. D.G.Chougule
Professor, E&TC Dept., T.K.I.E.T. Warananagar

ABSTRACT:

Video watermarking is the practice of inserting an encode information known as the watermark, into an original video in an imperceptible manner. The watermark encodes or represents information that can protect the watermarked video, typically identifying the owner (source) or the intended recipient (destination) of the video. The embedded watermark may be detected by using a watermark detector, which enables an application to react to the presence (or absence) of the watermark in a video. However, the watermarked video may be processed, or attacked, prior to watermark detection. Attacks may remove the embedded watermark or make the watermark more difficult to detect. Most watermark detectors will fail to detect the watermark embedded in the attacked video unless the position of the watermark can be identified. In order to overcome this limitation, a new multi-wavelet based video watermarking in tutorial videos has been proposed. Embedding and detection models are proposed that encompass the behaviour of many video watermarking techniques. The multi-wavelet transform uses two transformations such as Haar transform and Doubchies transform. The work is done with the help of designed user interface. This method extracts the secret message correctly and this provides better performance.

KEYWORDS: Multiwavelet Transform, Video Encoding, Haar transform and Doubchies transform.

INTRODUCTION:

The acquisition and distribution of multimedia like image, audios and videos have more easily with the rapid growth of computer and internet technology. Using media processing tools, the media data can be easily reproduced or get manipulated. Therefore the protection of the copyright of multimedia is an important topic now. Lots of techniques to protect the multimedia have been developed. They are used for several purposes as well as the copyright protection. Two basic methods of information hiding are cryptography and steganography. The term steganography means "cover writing" and the term cryptography means "secret writing". Cryptography is a widely used method for protecting the digital media. The message is encrypted before it gets transmitted and decrypt the message after it gets received using the key. No one can access the content without having the true key. The message is called the plain text and the corresponding encrypted message is called the cipher text. In cryptography, the message is protected before it gets transmitted. But after decryption, the information becomes unprotected and it can be copied and can spread to anybody. In steganography, the message is embedded into the digital media rather than encrypting it in such a way that nobody except the sender and the intended recipient can even realize that there is a hidden message. The digital media content that to be protected is called the cover can be determined by anybody, but the message hidden in the cover can be detected by only the person having the actual key. Thus this method relates to covering point-to-point communication between the two parties. Thus steganography are usually not robust against the modification of the data because it has only limited applications.

The success of the Internet, cost-effective and popular digital recording and storage devices, and the promise of higher bandwidth and quality of service for both wired and wireless networks have made it possible to create, replicate, transmit, and distribute digital content in an effortless way. The protection and enforcement of intellectual property rights for digital media has become an important issue [1]. Digital watermarking is the technology that provides and ensures security, data authentication and copyright protection.

Watermarking is considered as an optimistic technique to protect the copyright of the multimedia. The concept of digital watermarking is derived steganography. Digital watermarking is field that requires continuous efforts to find a way in protecting multimedia content. Watermarking technique embeds data into a multimedia object to protect owner's ownership to the object. The pattern of bits embedded into a digital image audio or video files that give the

copyright information. Digital watermarking also called as watermark insertion or watermark embedding, constitute the method of inserting information into multimedia data also called original data or cover data, The embedded information or the watermark can be a serial number or random number sequence, ownership identifiers, copyright messages, control signals, transaction dates, information about the creators of the work, bi-level or gray level images, text or other digital data formats. Video watermarking has become one of the most accepted watermarking techniques in recent years.

The term "digital watermarking" was first coined by Tirkel in 1993, when presented two watermarking techniques to hide the watermark data in the images [2]. It refers to embedding of signal, secret information (i.e. watermark) into the digital media such as image, audio and video. This is the first of the two modules of the watermarking process, termed as watermark embedding. In the second module, the embedded information is detected and extracted out to reveal the real owner/identity of the digital media, termed as extraction module [3]. Digital watermark can be used for copyright protection and authenticate the authorized of the video [4]. Its applications include copying prevention, broadcast monitoring, authentication and data hiding [3].Video watermarking is a quickly evolving field in the area of multimedia. As the copying the digital media has become comparatively easy, the society is contaminated by the enormous policy of digital data. Here the copyright protection must not be eroded due to the spiteful attack. Watermarking system may be visible or invisible. Invisible watermarking implies that the watermark is barely visible when the watermarked signal is displayed. Video watermarking techniques are generally divided into three groups: compressed domain methods, transform domain methods and spatial domain methods. Spatial domain method embeds the watermark signals into the chrominance or luminance components of the host video data. This method cannot resist the attack easily as they are very fast and simple method. The characteristics of the transform frequency domain are more robust, stable and invisible method when compared with the characteristics of the spatial domain method. Hence more video watermarking schemes are done based on the transform domain. There are many algorithms which exist to modify the original media to generate the watermarked media. Generally there may be no difference between the original media and the watermarked media. But in some case, there may be perceptible difference between the original media and the watermarked media.

DIFFERENT TYPES OF WATERMARKING METHODOLOGIES:

Lots of algorithms have been presented in the past for video watermarking. Algorithm used in image watermarking can be applied directly to the video watermarking therefore many algorithm of image watermarking is also used in video watermarking. Each and every algorithm has its advantages and disadvantages. In video watermarking, watermark is generally embedded in uncompressed video or some time in compressed video. In broader sense or in the basis of domain on which watermark is inserted, video watermarking can be grouped in to three different categories as shown in the figure 1.

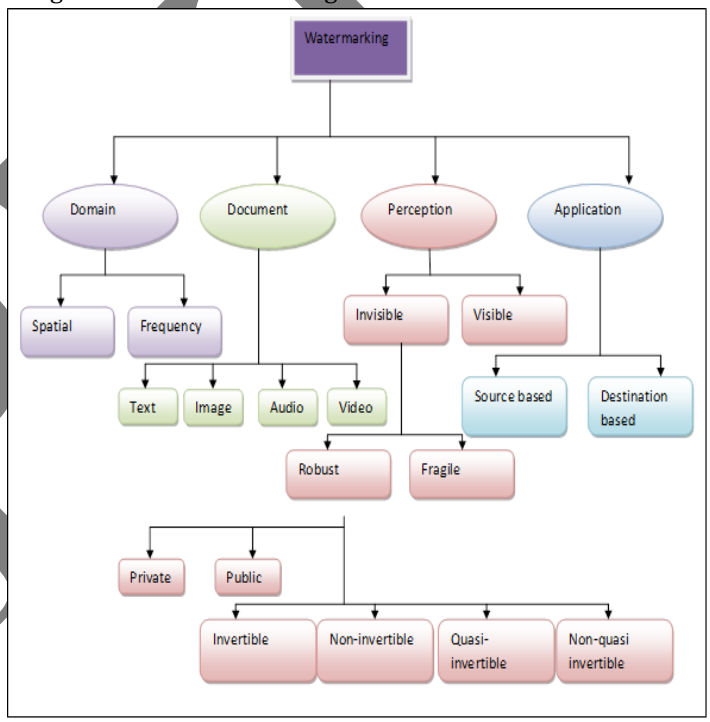

Figure 1: Different types of watermarking methodologies.

The watermarking technique is mainly divided into domain, document, perception and application. The spatial and frequency technique are domain category. The document subdivision is text, image, audio and video. The perception based watermarking is invisible and visible. The invisible types are robust and fragile. The robust type is either private or public. The fragile based perception is invertible, non-invertible, quasi-invertible and non-quasi invertible. The source based and destination based technique are under the application category. Spatial domain watermarking is performed by modifying the pixel color samples of a video frame where as the watermarks of frequency domain techniques are applied to the coefficients obtained as a result of frequency transform of either a whole frame or a single block-shaped regions of a frame. Discrete Fourier Transform (DFT) and Discrete Wavelet

Transform (DWT) belong to the whole frame frequency transform. Video sequences compressed by modern technique provide another type of domain, motion vectors. Watermarking in the domain vector moderately alters the direction of the motion vectors.

RESULTS:

The proposed multi-wavelet based video watermarking technique is done on the basis of two steps such as watermark embedding process and watermark extraction process. The secret message is inserted into the video with the help of a key is done through the process of watermark embedding. The same secret message can be extracted with the help of the corresponding key through the process of watermark extraction.

The watermark extraction process mainly includes two steps such as watermark embedding and watermark extraction. Both the embedding and extraction process includes some steps such as shot segmentation, frames extraction and multi-wavelet transformation. From these steps, some frames of the video are extracted for further processing.

The main facilities available for the video watermarking is,

- MATLAB R2013a with updated Toolboxes
- Processing Machine with at least
  - 2GB RAM
  - Dual core processor
  - GHz clock speed and
  - 32 – bit Windows Operating system

Figure 2: Sample tutorial video images

Some of the sample images from the video are shown in figure 2. The input is nothing but the video. The sample images describe the some frames which are obtained from the video.

USER INTERFACE:

Video watermarking with authentication for tutorial videos using multi-wavelet are done with the help of designed user interface. The user interface used in this work is shown in figure 2.

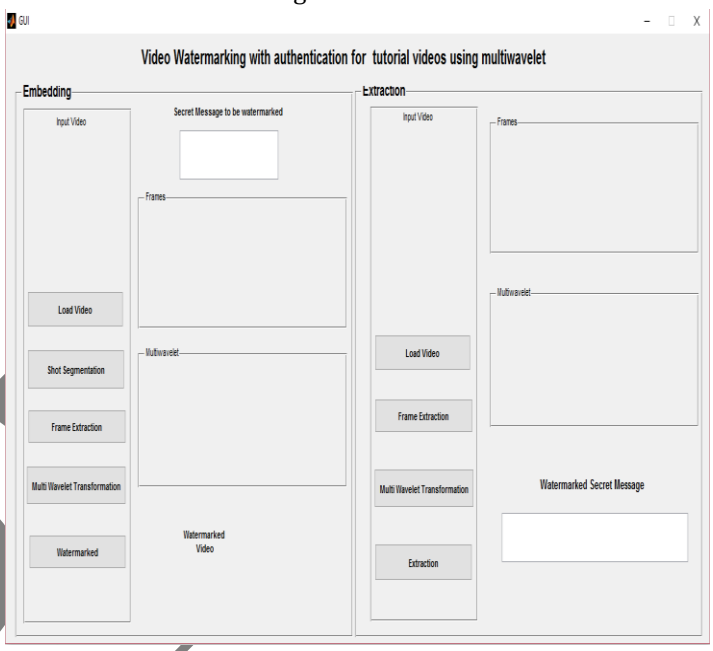

Figure 3: Designed User Interface for video watermarking

The user interface consists of two main blocks such as embedding and extraction. The embedding block contains the keys such as

- input video
- load video
- shot segmentation
- frame extraction
- multi-wavelet transformation
- secret key message box

The input video contains the video in which the watermark is to be embedded. The load video key is used for loading the input. While loading input video, the corresponding video will be displayed in the input box. Then the secret message is inserted in the block which shows secret message to be watermarked. Then the shot segmentation button will provide the shot segmented output. The frame extraction and multi-wavelet transformation provides the result with some features in the video. Before that it will ask the secret key, and we should enter the secret key. So the watermarked video will obtain in this section.

In extraction process, the same procedure is carried out. Here while loading the input the watermarked video is loaded. After the wavelet transformation process, the corresponding key should be entered. Then the

corresponding message will display in this section. I we enter the wrong key, Then it shows the warning as the key does not match.

After the tutorial video watermarking embedding process and extraction process, the performance measures are measured for this work. Here we consider a parameter for the evaluation of this work. The parameter used is Peak Signal to Noise Ratio for fidelity measurement. The tabular column for the performance is shown in Table I.

Cases	Proposed Multi-wavelet transformation	Haar transform	Doubchies transform
Message 1	43.20 dB	25.65 dB	35.66 Db
Message 2	46.00 dB	29.45 dB	34.78 dB
Message 3	40.98 dB	24.76 dB	31.87 dB
Message 4	39.87 dB	25.45 dB	39.88 dB
Message 5	46.88 dB	27.65 dB	36.76 dB

Table I: Performance Analysis on the Video Watermarking For Different Messages

In Table I, it describes the PSNR value for the proposed watermarking technique for the tutorial videos. Peak signal-to-noise ratio, often abbreviated PSNR, is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. Because many signals have a very wide dynamic range, PSNR is usually expressed in terms of the logarithmic decibel scale. Here the comparison is performed for the proposed work, Haar transform and Daubechies transform. Here the proposed work provides better performance than other transform. Moreover, the performance of Daubechies transform is better than the Haar transform. The comparison is done for 5 different images and it shows different PSNR values.

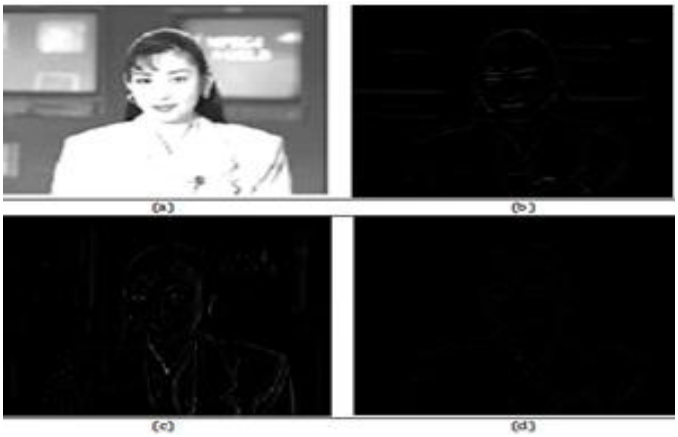

Figure 4: Output From Haar Wavelet Transformation On The Actual Frame (A), (B), (C) And (D) Are Different Components From Wavelet Outcomes.

The multi-wavelet transformation is carried out after loading input video followed by shot segmentation and frames extraction. It is carried out by two wavelet transformation such as Haar transformation and Doubchies transformation.

In the Haar transform, frames extracted will not be clear. The diagram clearly shows that the frames are not displaying clearly.

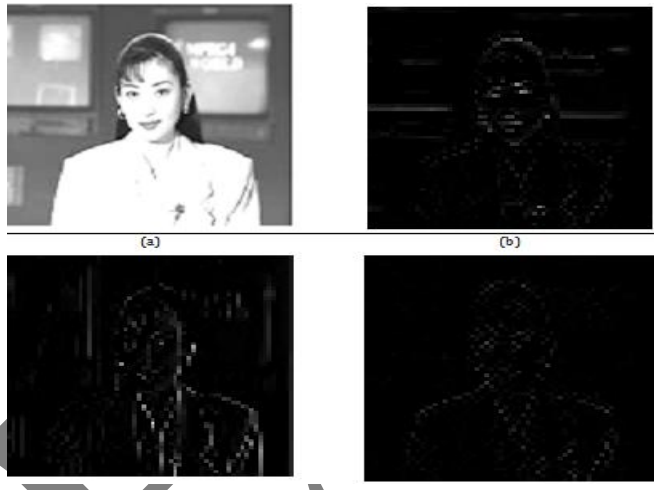

Figure 5: Output of Doubchies transformation on the frames from Haar transformation, (a), (b), (c) and (d) are different components from wavelet outcomes

In the diagram the output of Doubchies transformation is better than the Haar wavelet transformation. I shows some of the features of the video slightly. So here Haar transformation followed by Doubchies transformation is better in this video watermarking.

EXPERIMENTAL RESULTS OF TUTORIAL VIDEO WATERMARKING:

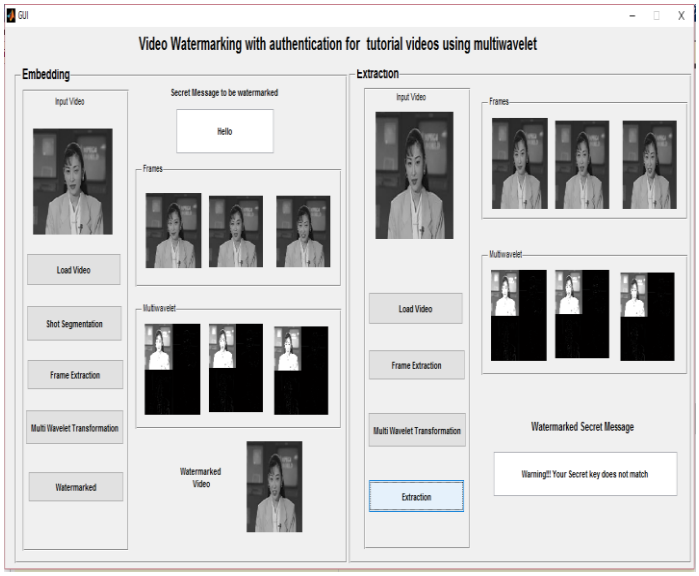

Figure 6: Experimental results of tutorial video marking

While processing, the secret key is inserted initially. So while extracting the message, the corresponding key should be entered. If we enter the

correct key, the message will display. But if we enter the wrong key, a warning message will display as the secret key does not match.

CONCLUSION:

Watermarking is a copy protection system that allows tracking back illegally produced copies of the protected multimedia content. Compared with other copy protection systems like Digital Rights Management, the main advantage of watermarking is that the watermark is embedded permanently in visual data of the content but at the cost of slight loss in fidelity. Unless the position of the watermark can be identified, most watermark detectors will fail to detect the watermark embedded in the attacked video. This paper is based on video watermarking in tutorial videos. In order to overcome some limitations in video watermarking techniques, a new method which consists of shot segmentation, frames extraction and multi-wavelet transformation. The multi-wavelet transformation uses two types of transformations such as Haar and Doubchies transformations. The Haar transform extracts only some frames in the video. So here Doubchies transform is used to extract frames more than that. The extracted frames are used fro further processing with the help of designed user interface. Thus this method provides better result when compared with other existing methods.

REFERENCES:

[1] C. I. Podilchuk, and E. J. Delp, "Digital watermarking: Algorithms and applications", *IEEE Signal processing Mag., vol. 18, no. 4, pp. 33-46, 2001.*

[2] R. G. Van Schyndel, A. Z. Tirkel, and C.F Osborne, "A Digital Watermark", in Proc. *IEEE Int. Conf. Image Processing, ICIP-1994, Austin, TX, vol.2, pp. 86-90, 1994.*

[3] P. Singh, and R. S. Chadha "A Survey of Digital Watermarking Techniques, Applications and Attacks", Int. *J. Engg.and Innovative Technology (IJEIT), vol. 2, no. 9, pp. 165-175, 2013.*

[4] J. Panyavaraporn, "Multiple video watermarking algorithm based on wavelet transform", in *Proc. 13th Int. Sym. Comm. and Information Technologies (ISCIT), SuratThani, pp. 397-401, 2013.*

[5] J. Li, P. Zhong, Y. Zhu, and C. Guo, " Robust wavelet-based watermarking scheme for video copyright protection", in *Proc. 7th Int. Congress on Image and Signal Processing (CISP), Dalian, pp. 125-129, 2014.*

[6] R. Lancini, F. Mapelli, and S. Tubaro, "A robust video watermarking technique in the spatial domain", in *Proc. 8th IEEE Int. Sym. Video/Image Processing and Multimedia Comm., pp. 251–256, 2002.*

[7] D. W. Xu, "A Blind Video Watermarking Algorithm Based on 3D Wavelet Transform", in *Proc. Int. Conf. Computational Intelligence and Security, Harbin, pp. 945-949, 2007.*

[8] A. Koz, and A. A. Alatan, "Oblivious spatio-temporal watermarking of digital video by exploiting the human visual system", *IEEE Trans. Circuit and Systems for Video Technology, vol. 18, no. 3, pp. 326-337, 2008.*

[9] M. Asikuzzaman, M. J. Alam, A. J. Lambert, and M. R. Pickering, "Imperceptible and Robust Blind Video Watermarking Using Chrominance Embedding: A Set of Approaches in the DT CWT Domain", *IEEE Trans. Information Forensics and Security, vol. 9, no. 9, pp. 1502-1517, 2014.*

[10] G. C. Langelaar, and R. L. Lagendijk, ''Optimal Differential Energy Watermarking of DCT Encoded Images and Video", *IEEE Trans. Image Processing, vol. 10, no. 1, 2001, pp. 148-158, 2001.*

[11] T. Sun, X. Jiang, S. Shi, Z. Lin, and Guanglei Fu, "A Novel Self-adaptation Differential Energy Video Watermarking Scheme in Copyright Protection", *J. Multimedia, vol. 4, no. 3, pp. 153-160, 2009.*

[12] A. Mansouri, A. M. Aznaveh, F. T. Azar and F. Kurugollu, "Low Complexity Video Watermarking in H.264 Compressed Domain", *IEEE Transactions on Information Forensics and Security, vol. 5, No. 4, pp. 649-657, 2010*

[13] C. S. Lu, and H. Y. M. Liao, "Video Object-based Watermarking: A Rotation and Flipping Resilient Scheme", in Proc. IEEE *Int. Conf. Image Processing, IEEE Press, vol. 2, pp. 483-486, 2001.*

[14] Y. Wang, and A. Pearmain, "Blind MPEG-2 Video Watermarking Robust Against Geometric Attacks: A Set of Approaches in DCT Domain", *IEEE Trans. Image Processing, vol. 15, no. 6, pp. 1536-1543, 2006.*

[15] L. Wang, H. Ling, F. Zou and Z. Lu, "Real-Time Compressed- Domain Video Watermarking Resistance to Geometric Distortions", *IEEE Multimedia, vol. 19, no. 1, pp. 70-79, 2012*