ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 2, August 2012

An Innovative Fusion Technique for Secured Video Watermarking

Nirmal S.C, Dr.B.Parthasarathy

Abstract*— Digital Watermarking technique has been proposed as a method to hide secret information into the signals so as to discourage unauthorized copying or attest the origin of the media. A number of video watermarking techniques are proposed. These techniques exploit different ways in order to embed a robust watermark and to maintain the original video signal fidelity. This paper proposes a fusion technique of using different techniques in a single frame using Octic Group Permutation.

***Index Terms*— Digital Video Watermarking, Copyright Protection, D.C.T, D.W.T, D.F.T.**

I. INTRODUCTION

The idea of communicating secretly is as old as communication itself. In this age of Data blaze, the data communication is also snooping for new ideas of Secret and secured data communication. The advantage of digital media components such as Internet, C.D.ROMs, Pen drives and Memory sticks etc lies in the fact that the duplication, distribution and modification of contents are much earlier than the older Media, such as printed Media. So replication of a digital content can be performed lacking any trouncing of its quality. These advantages; however are double edged swords. With the ease of editing and perfect reproduction in digital domain, the protection of ownership and the prevention of unauthorized tampering of multimedia data become important concerns. Traditionally Encryption and control access techniques like Cryptography and Steganography were employed to protect the ownership of media. These techniques however do not protect against unauthorized copying after the media have been successfully transmitted and decrypted. Naturally, this situation has raised many concerns about probable defiance of Intellectual Property Rights (I.P.R). Unauthorized duplication and distribution of copyrighted material (photographs, music, movies, etc.), devoid of appropriate compensation to the copyright holders, are becoming increasingly problematic. Devoid of deciphering this security concern, digital multimedia products and services cannot take-off in an e-commerce setting.[1] There are two basic kinds of copyright marks: Fingerprints and Watermarks. A Fingerprint is an embedded serial number while a watermark is an embedded copyright message. The first enable us to trace offenders, while the second can provide some of the evidence needed to prosecute them. Data embedding or (digital) watermarking, put structures called watermarks into digital contents, in such a way that the structures do not interfere with intended use of the contents. Watermarking is a concept of embedding a special pattern, a watermark into a Multimedia document, so that a given piece of copyright information is permanently tied to the data [2]. A watermarking system is made up of a watermark embedding system and a watermark recovery system. Watermarking has been considered to be a promising solution to protect the copyright of multimedia data through transcoding, because the embedded message is always included in the data. The basic components of any watermarking technique consist of a marking algorithm that inserts information - the watermark - into an image, and a verification algorithm that detects if or how much of the watermark remains in the image under test. Image watermarking is in an exhaust state, and the focus of research spotlight is now fully on Video stuffs. Video watermarking has been initially approached as direct extension of still image watermarking, with time constraint i.e. by considering a video as a set of still images, which are individually protected. But recent studies reveal that, more focus has to be given on it to make the technique of watermark embedding robust. The following points can be abstracted out as some of them.

a) Between the frames there exists a huge amount of Intrinsically redundant data.
b) There must be a strong balance between the motions and The motionless regions.
c) Strong concern must be put forth on real time and Streaming video applications.

II. VIDEO WATERMARKING TECHNIQUES

Watermark can be either directly inserted in the raw video data or integrated during encoding process or implemented after compressing the video data. According to the Domain of application, Watermarking can be divided into Spatial Domain and Frequency Domain. Early researches prove that Frequency domain based transformations are more robust than the former one. Basic Frequency Based transformation techniques are,

1. Discrete Cosine Transformation
2. Discrete Wavelet Transformation
3. Discrete Fourier Transformation

A number of solutions have been proposed where frequency sensitivity of Human Visual System is exploited to ensure that the watermark is imperceptible. Those solutions

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 2, August 2012

use transform domain and the watermark is added directly into the transform coefficients of the image. More advanced embedding algorithms have been created by taking full advantage of characteristics of the HVS. A number of solutions have been proposed where frequency sensitivity of HVS is exploited to ensure that the watermark is imperceptible. Those solutions use transform domain and the watermark is added directly into the transform coefficients of the image. More advanced embedding algorithms have been created by taking full advantage of characteristics of the HVS. Alexander Sverdlov et.al proposed a method of watermarking by dividing the image into four quadrants and embedding using DCT and DWT domains [3]. Recent works [4, 5] indicates that embedding a watermark in low frequencies is robust to one set of attacks whereas embedding a watermark in high frequencies is robust to another set of attack.

III. The Innovative Fusion Method of Watermarking

Here the video clips are segmented into frames. Each, such frame is divided into four quadrants. These four quadrants are to be embedded with these three transformations technique. So for each frame one technique have to be doubled. These doubling technique have to be chosen with a simple permutation technique, for each such frame. Now the order of embedding of each such technique is determined using an Octic Group Permutation. These frame quadrants are permuted in the way of Group of Symmetry of the Square (Octic Group) using ρ_i for rotations, μ_i for mirror images in perpendicular bisectors of sides and δi for diagonal flips. There are eight permutations involved here.

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \quad \mu_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \quad \mu_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \quad \mu_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \quad \mu_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$$

where 1 denotes D.F.T , 2 denotes D.C.T, 3 denotes D.W.T and 4 denotes the one which is selected using simple permutation. Thus the watermarking schemes are rotated randomly using these Octic Group permutation methods, so as to make the watermarking scheme robust. As in this case of watermarking, when a watermarked video is attacked, any of the or part of the watermark in each frame may still survive. As the watermarks are embedded in different domains, they can compensate each other in resisting against different attacks. Nevertheless, different watermarking schemes may also affect each other when under attacks.

IV. Algorithm

Step 1: Preprocess the Video sequence by segmenting it into frames. For each frame, do this,

Step 2: Apply separable 2D Wavelet Transform to Decompose the cover host frame into four levels Sub-bands to produce a low – frequency sub-band LL_4, and three series of high frequency sub-bands: HL_j, LH_j and HH_j where $j<4$

Step 3: Assign each of the techniques we use, i.e. DWT, DFT, DCT numbers respectively as 1, 2, 3

Step 4: Apply Permutation to get one technique from these three techniques. This selected technique is used Twice in this frame.

Step 5: Apply Octic Group permutation to get a sequence for Embedding order, on each quadrant of a single frame.

Step 6: Decompose the frame first to the needed transform Domain, embed the watermark, then inverse transform; to do it again with the next transformation technique.

Step 7: Inverse transform to get the watermarked frame.

V. Results

The result of video clips watermarked with this fusion method, even after attacks, shows a very good robustness factor. The performance of the new Video Watermarking scheme is evaluated through several experiments; Analysis test using Stirmark4 test. Normalized co-relation is calculated using,

$$NC = \frac{\sum_{i=0}^{N-1}\sum_{j=0}^{N-1} W(i,j)\,\acute{W}(i,j)}{\sum_{i=0}^{N-1}\sum_{j=0}^{N-1} [W(i,j)]^2}$$

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 2, August 2012

The final result shows a very good robustness toward many of the known attacks like Lossy Compression, Cropping, Re-Scaling etc

VI. Conclusion

The Discrete Wavelet Transform (DWT), The Discrete Cosine Transform (DCT) and The Discrete Fourier Transform (DFT) have been applied successfully in many in digital Video image watermarking. But in this paper, we described a fusion technique which combines all these techniques in a single frame.Since different techniques are fused in a single frame and the order of these applications get changed frame after frame, a single method attack will not tamper the watermark fully, as a technique to tamper a specified technique may not be a menace for another one and viz. So the new method of fusion technique founds to be a hefty technique for video systems to copyright.

REFERENCES

[1] K. Su, "Digital Video Watermarking Principles for Resistance to Collusion and Interpolation Attacks," Master of Applied Science thesis, University of Toronto, Sept. 2001.

[2] F.A.P. Petitcolas, R.J. Anderson, M.G. Kuhn: "Information Hiding - A Survey", Proc. of IEEE, pp.1062-1078, July, 1999..

[3] Alexander Sverdlov, Scott Dexter , Ahmet M.Eskicioglu " Secure DCT-SVD Domain Image Watermarking : Embedding Data in All Frequencies" Paper presented in Image Processing Seminar at Brooklyn College, N.Y , Oct 23- 26,2006

[4] R. Mehul and R. Priti, "Discrete Wavelet Transform Based Multiple Watermarking Scheme," Proceedings of IEEE Region 10 Technical Conference on Convergent Technologies for the Asia-Pacific, Bangalore, India, October 14-17, 2003.

[5] P. Tao and A. M. Eskicioglu, "A Robust Multiple Watermarking Scheme in the Discrete Wavelet Transform Domain," Optics East 2004 Symposium, Internet Multimedia Management Systems V Conference, Philadelphia, PA, October 25-28, 2004.

[6] Ali Al-Haj, "Combined DWT-DCT Digital Image Watermarking", Journal of Computer Science 3 (9): 740-746, 2007 ISSN 1549-3636.

[7] Kesavan Gopal and Dr. M. Madhavi Latha, "Watermarking of Digital Video Stream for Source Authentication" , IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 4, No 1, July 2010 , ISSN (Online): 1694-0784 ISSN (Print): 1694-0814.

[8] Rashmi Agarwal K. Venugopalan "Digital Watermarking of Color Images in the Singular Domain" IJCA Special Issue on "Computational Science - New Dimensions & Perspectives" NCCSE, 2011.

[9] V.Santhi and Dr. Arunkumar Thangavelu "DWT-SVD Combined Full Band Robust Watermarking Technique for Color Images in YUV Color Space" International Journal of Computer Theory and Engineering, Vol. 1, No. 4, October 2009.

[10] T.L. Wu, S.F. Wu, " Selective encryption and watermarking of MPEG video" ,International Conference on Image Science, Systems, and Technology, CISST'97,June 1997.