International Journal of Scientific & Engineering Research, Volume 5, Issue 4, April-2014
ISSN 2229-5518

A Survey On Effective Video Watermarking Techniques Using Quantization Index Modulation

Kumari Subhadra Otta, Sushree Satvatee Swain

Abstract—Modern challenges and accelerating growth in internet and technology leads to increase in the data swap and use of digital media. Hence, there is a need of copyright protection of the digital media. Digital video watermarking is a modern and widely used technique for protecting the digital media by embedding the additional data along with the video signal. A number of video watermarking techniques are proposed. In this review paper, the Pseudo 3D-DCT technique is applied where DCT transformation is taken twice i.e. 2D-DCT is applied to image plane and again 1D-DCT is applied to time axis .Again the watermark is embedded in the quantized regions of related frames and the result obtained as secret embedding key is further applied for extraction.

Index Terms—Block matching, Domain watermarking, HVS model, Pseudo 3D-Discrete cosine transform(DCT),Pseudorandom generator, Quantization Index Modulation.

INTRODUCTION

Watermarking one is hiding a message signal into a host signal, without any perceptual distortion of the host signal. As the word "watermarking" suggests, the mark itself is "transparent" or unnoticeable for the human perception system. Usually, the host signal is a digital media, like audio, video or images. As we all know, the Human Visual System (HVS), is far from being perfect and for images/video it is possible to modify the pixel values without the watermark being visible. Providing that a certain HVS threshold is not exceeded, the modified (watermarked) image/video will be undistinguishable to the human eye compared with the original .

I. Classification of watermarks

The watermark is classified into Fragile & Robust. The Fragile watermark which refers to discover the minor changes in any image, while the robust one is specially designed to withstand a wide range of "attacks", which basically are trying to remove the watermark, but without destroying the image/video. So, the pictorial classification of watermarking has been presented.

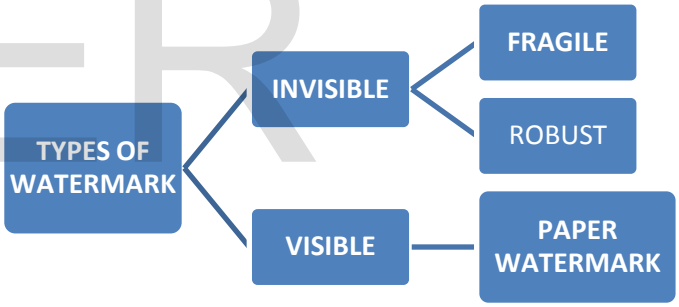

Figure 1: Types of watermark

In the above figure a watermark can be added to the uncompressed data (raw data), such as a standard uncompressed video sequence as described by ITU-R 601, or can be added to the compressed bit-stream (MPEG2).

II. Description of Domain watermarking

There are two type of domain marking.

(a)Spatial domain

Kumari Subhadra otta and Sushree satvatee swain are with the Department of Electronics & communication Engineering, Kalinga Institute of Industrial Technology, Bhubaneswar-751204, India (e-mail: subhadra.otta@gmail.com) (ssatvatee16@gmail.com).

(b)Frequency domain

The easiest way to watermark an image/video, is to change directly the values of the pixels, in the spatial domain. A more advanced way to do it, is to insert the watermark in the frequency domain, using one of the well known transforms: FFT, DCT or DWT.

The watermark embedding can be done uniformly (or in some other empirical manner), which doesn't account for the HVS properties (this is called non-perceptual marking). Or, the watermarking embedding can use some HVS models in order to optimise the embedding. Depending on the HVS model used, the perceptual marking can be video independent (basic HVS model) or preferably video dependent (advanced HVS model).

III. Preface to the Video watermarking System

The watermark embedding : the original video is watermarked with a binary sequence of 64 data-bits, using a secret key, resulting the watermarked video.

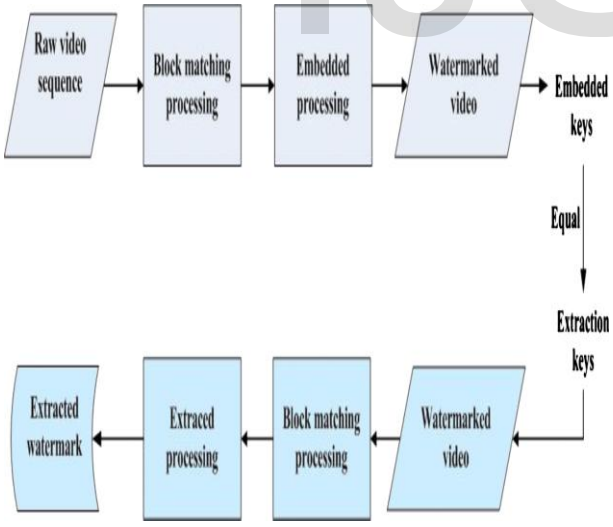

Figure 2: Watermarking process

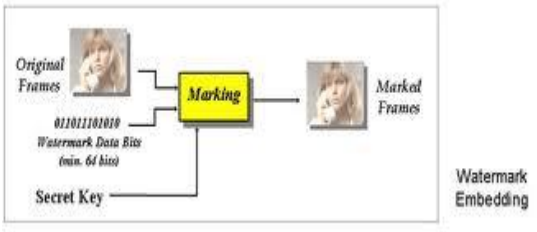

Figure 3: Watermark embedding

The watermarked video is now in the distribution channel. In the distribution channel all the data are to be sent. Here one could try to attack the watermark, in order to destroy it. For example, a pirate who wants to breach the intellectual property rights of the real owner, has all the interest to "remove" the watermark. In this case the attacks are intentional. It is important to mention here, that the intentional attacks must not alter too much the video sequence, because the attacker still wants to use it, and a bad quality video sequence is worthless. Some examples of intentional attacks are: the geometric attacks, frame dropping, collusion, etc.

A different class of attacks are those qualified as unintentional, for example those caused by typical processing in the video chain and during transmission of the video signal. Finally, the watermarking retrieval, which is the most difficult part of the system, has to recover the watermark.

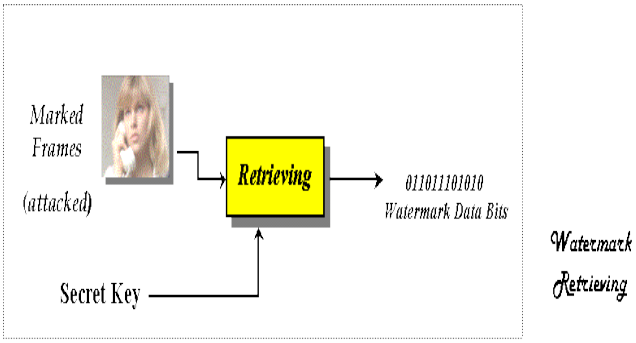

Figure 4:Watermarking retrieval

Kumari Subhadra otta and Sushree satvatee swain are with the Department of Electronics & communication Engineering, Kalinga Institute of Industrial Technology, Bhubaneswar-751204, India (e-mail: subhadra.otta@gmail.com) (ssatvatee16@gmail.com).

IV RELATED TECHNIQUES

There are three categories for existing video watermarking techniques. The domain watermarking categories are shown below in the figure 5.

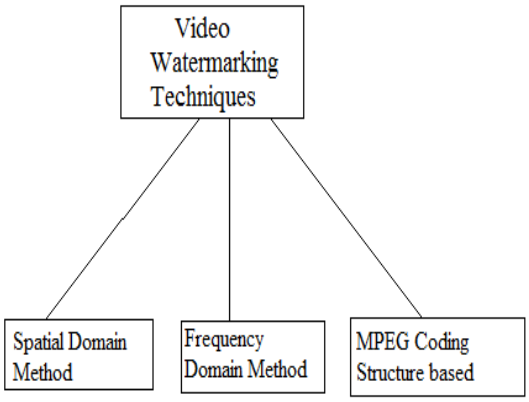

Figure 5: Classification map of existing digital video watermark techniques

A. Spatial Domain Watermarking:-

The spatial domain watermarking techniques embed the watermark by modifying the pixel values of the host image/video directly. Low computational complexities and simplicity are the main strengths of pixel domain methods. For better performance in real time these techniques are more attractive.

- *Least Significant Bit Modification :-*

  In this technique, the Least Significant Bit of each pixel is used to embed the watermark or the copyright information. In this technique cover image is used to store the watermark, in which we can embed a smaller object multiple times. The pixels are identified where embedding will be done using a pseudo-random number generator based on a given key.

  LSB modification is suitable tool for steganography as it is a simple and powerful tool for it. But it cannot preserves robustness which is required in watermarking applications.

- *Correlation-Based Techniques :-*

  The most straightforward way to add a watermark to an image in the spatial domain is to add a pseudo random noise pattern to the luminance values of its pixels. A Pseudo-random Noise (PN) pattern W (x, y) is added to the cover image I (x, y), according to the given below:

  $I\,w\,(x, y) = I\,(x, y) + k\,*W\,(x, y)$

  Where k denotes a gain factor and Iw the watermarked image. The robustness of the watermark is increased by increasing the value of k at the expense of the quality of the watermarked image. The same key is given as an input to retrieve the watermark, to the same pseudo-random noise generator algorithm, and the correlation between the noise pattern and possibly watermarked image is computed. If the correlation exceeds a certain threshold T, the watermark is detected, and a single bit is set . This method can easily be extended to a multiple-bit watermark by dividing the image into blocks and performing the above procedure independently on each block.

B. Frequency Domain Watermarking

Most of watermarking techniques ,the watermark will be embedded into the frequency domain instead of the spatial domain for the robustness of the watermarking mechanism. Discrete Cosine Transformation (DCT), Discrete Fourier Transformation (DFT) and Discrete Wavelet Transformation (DWT) are the three main methods of data transformation in this domain. The main strength offered by transforming domain techniques is that they can take advantage of special properties of alternate domains to address the limitations of pixel-based methods or to support additional features. Generally, transform domain methods require higher computational time.

- *Discrete Fourier Transform :-*

  This approach first extracts the brightness of the to-be-marked frame, computing its full-frame DFT and then taking the magnitude of the coefficients. The watermark is composed of two alphanumerical strings. The DFT coefficient is

Kumari Subhadra otta and Sushree satvatee swain are with the Department of Electronics & communication Engineering, Kalinga Institute of Industrial Technology, Bhubaneswar-751204, India (e-mail: subhadra.otta@gmail.com) (ssatvatee16@gmail.com).

altered, then IDFT. Only the first frame of each GOPs is watermarked, which was composed of twelve frames, leaving the other ones uncorrupted. It is good robustness to the usual image processing as linear/non-linear filtering, sharpening, JPEG compression and resist to geometric transformations as scaling, rotation and cropping.

- *Discrete Cosine Transform :-*

  The following are steps carried out in the encoding procedure of DCT:

  1. The image is broken into N*N blocks of pixels.

  2.In matrix multiplication the DCT is applied to each block from left to right, top to bottom.

  3. Each block's element is compressed through quantization means dividing by some specific value. Quantization is achieved by dividing each element in transforming image matrix by the corresponding element in quantization matrix.

  4. The array of compressed blocks which represent the image is stored in a reduced amount of space. It is carried out using zigzag sequences.

- *Discrete Wavelet Transform*

  The DWT decomposes an input image into four components namely LL, HL, LH and HH where the first letter corresponds to applying either a low pass frequency operation or high pass frequency operation to the rows, and the second letter refers to the filter applied to the columns. signal are largely confined to the high frequency part. The low frequency part is split again into two parts of high and low frequencies. This process is continued an arbitrary number of times, which is usually determined by the application at hand

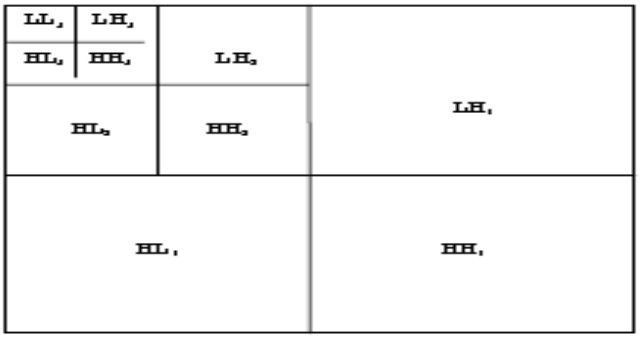

Figure 6 . The Model of DWT decomposition

In the encoding part of DWT while watermarking, we first decompose an image into several bands with a pyramid structure as shown in Fig. above and then add a pseudo-random sequence (Gaussian noise) to the largest coefficients which are not located in the lowest resolution.

C. Contourlet Transform (CT) :

DWT offers multistage and time frequency localization of the image. However, it fails to represent the image effectively, if the image contains smooth contours in different directions. CT addresses this problem due to its inherent characteristics, viz., directionality and anisotropy[1]

The DCT based algorithm for watermarking and monitoring video streams in a TV-broadcasting environment survives mpeg-2 compression of high-quality, real-world video sequences without degrading their quality. Applying the algorithm to fast-moving synthetic video sequences requires much longer time-integration intervals than the 50-frames-wide window The algorithm's current version is well suited for watermarking digital video streams such as movies or sporting events. The format of digital video is restricted to some well defined geometry. This makes geometric distortions detectable and removable. To introduce geometric distortions, an attacker would have to decode the video stream, process it, and encode it again.

Kumari Subhadra otta and Sushree satvatee swain are with the Department of Electronics & communication Engineering, Kalinga Institute of Industrial Technology, Bhubaneswar-751204, India (e-mail: subhadra.otta@gmail.com) (ssatvatee16@gmail.com).

Thus, because pirates must attack the watermark in real time, the cost of the attack increases. Future work will focus on the reconstruction of the original geometry of distorted watermarked video frames and more elaborate time integration methods. This proposed method was not robust against mpeg-4 [2][3]

Other scheme uses digital watermark embedding scheme based on DCT transform and Image scrambling and aim MPEG4 at embedding watermark information. MPEG4, the standard for DVD, is widely used in industry. the carrier is MPEG4 video with the size of about 10M. And watermark information is a binary image. using DCT transform can save computing time and is more robust. Before watermark is embedded, scrambling image is adopted to transform watermark information .Also, the embedding position of the watermark bit is modified by one chaos sequence, and this method promotes the robustness and the security of the watermark. So unauthorized person cannot extract or remove the watermark because the embedding position is unknown.[4]

There should be no difference between watermarked and original signal, and the watermark should be difficult to remove without damaging the host signal. Two techniques for real time embedding of compressed video (i) adds the watermark by modifying the fixed length and variable length codes in the compressed video bit stream. It's drawback is it removes the watermark completely while decoding the bit stream (ii)adds the watermark by enforcing energy differences between various video regions but here watermark is still present even after decompressing video.[5]

Another method developed a watermarking algorithm based on the discrete cosine transform (DCT) and image segmentation. The image is first segmented in different portions based on the Voronoi diagram and features extraction points. Then, a pseudorandom sequence of real numbers is embedded in the DCT domain of each image segment. Different experiments are conducted to show the performance of the scheme under different types of attacks. The results show that the proposed watermark scheme is robust to common signal distortions, including geometric manipulations. The robustness against Joint Photographic Experts Group (JPEG) compression is achieved for a compression ratio of up to 45, and robustness against average, median, and Wiener filters is shown for the 3*3 up to 9*9 pixel neighbourhood. It is observed that robustness against scaling was achieved when the watermarked image size is scaled down to 0.4% of its original size.[6]

Even another scheme also worked on the image compression & signal processing technique which is produced by singular values decomposition. In SVD the position of the modified singular values is necessary. a novel SVD based blind video watermarking algorithm is proposed. Considering the visible quality and robustness, the watermarks are embedded in specially selected singular values, The matrix and its transpose have the same non-zero singular values.(i) The matrix and its row-flipped or column-flipped have the same non-zero singular values.(ii) The non-zero singular values of matrix are the
constant ratios to its scaled matrix (which is row or column repeated several times).The original order should be maintained for blind SVD based video watermarking[7]

Another scheme has been proposed which the watermark is embedded in larger value motion vectors, and specially in the less phase angle changed component. Then, the motion vector is modified into a new bit stream from which the watermark information can be easily retrieved. From the experimental results, it indicates that to embed watermark in motion vector has the advantage of little degrading the video quality, little influence on the MPEG decoding speed, capability to embed watermark in a short video sequence, and can be used to watermark on both the uncompressed and compressed video sequence.[8]

The problem of embedding one signal (e.g., a digital watermark), within another "host" signal to form a third, "composite" signal. The

Kumari Subhadra otta and Sushree satvatee swain are with the Department of Electronics & communication Engineering, Kalinga Institute of Industrial Technology, Bhubaneswar-751204, India (e-mail: subhadra.otta@gmail.com) (ssatvatee16@gmail.com).

embedding is designed to achieve efficient tradeoffs among the three conflicting goals of maximizing information-embedding rate, minimizing distortion between the host signal and composite signal, and maximizing the robustness of the embedding. A new classes of embedding methods, termed quantization index modulation (QIM) and distortion-compensated QIM (DC-QIM), and develop convenient realizations in the form of what we refer to as dither modulation. Using deterministic models to evaluate digital watermarking methods, we show that QIM is "provably good" against arbitrary bounded and fully informed attacks, which arise in several copyright applications, and in particular, it achieves provably better rate distortion–robustness tradeoffs than currently popular spread-spectrum and low-bit(s) modulation methods. Furthermore, we show that for some important classes of probabilistic models, DC-QIM is optimal (capacity-achieving) and regular QIM is near-optimal. These include both additive white Gaussian noise (AWGN) channels, which may be good models for hybrid transmission applications such as digital audio broadcasting, and mean-square-error-constrained attack channels that model private-key watermarking applications.

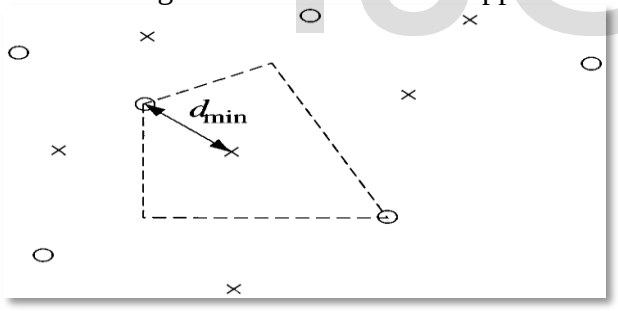

Figure 7: QIM for information embedding

The points marked with X's and O's belong to two different quantizers, each with its associated index.

The minimum distance 'd' measures the robustness to perturbations, and the sizes of the quantization cells, one of which is shown in the figure, determine the distortion.

If m = 1, the host signal is quantized to the nearest X. If m = 2, the host signal is quantized to the nearest O. Here the amplitudes of one single pixel or of a vector of pixels are quantized using one of a series of quantization lattices, chosen accordingly to the symbol to be embedded.[9]

Due to this above scheme of QIM a novel technique that is shown by construction to be insensitive to amplitude scaling, named Angle QIM (AQIM). Instead of embedding information by quantizing the amplitude of pixel values, AQIM works by quantizing the angle formed by the host-signal vector with respect to the origin of a hyper spherical coordinate system. This proved that AQIM method is insensitive to amplitude scaling attacks except when the watermarked image is completely erased.[10]

The combination of whole procedures gives result into a process of video watermarking where Pseudo 3d-dct & QIM is used[11].This is robust against various attacks. The watermark is mainly inserted into the uncompressed domain by adjusting the correlation between DCT coefficients of the selected blocks, and the watermark extraction is blind. This approach consists of a pseudo-3-D DCT, watermark embedding, and extraction. A pseudo-3-D DCT, which is taken DCT transformation twice, will be first utilized to calculate the embedding factor and to obtain the useful messages. Using the QIM, we embed the watermark into the quantization regions from the successive raw frames in the uncompressed domain and record the relative information to create a secret embedding key. This secret embedding key will further apply to extraction.

FUTURE WORK

Geometric attack robustness will be future work. This attack are not aimed at removing the watermark, but try to either destroy it or disable its detection. They attempt to break the correlation detection between the extracted and the original watermark sequence, where the

Kumari Subhadra otta and Sushree satvatee swain are with the Department of Electronics & communication Engineering, Kalinga Institute of Industrial Technology, Bhubaneswar-751204, India (e-mail: subhadra.otta@gmail.com) (ssatvatee16@gmail.com).

image is subjected to translation, rotation, scaling and/or cropping. This can be accomplished by "shuffling" the pixels. The values of corresponding pixels in the attacked and the original image are the same. However, their location has changed. These attacks can be subdivided into attacks applying general affine transformations and attacks based on projective transformation. Cropping is a very common attack since in many cases the attacker is interested in a small portion of the watermarked object, such as parts of a certain picture or frames of video sequence. With this in mind, in order to survive, the watermark needs to be spread over the dimensions where this attack takes place.

The problems which are occurring with signals, watermark should be a high shield in nature so that it would prove protective from getting attacked i.e. the technique would be robust against attacks.

ACKNOWLEDGMENT

We would like to thank all the authors mentioned in the references for their valuable work whose paper we have referred to do this survey.

REFERENCES

1. "Review on digital video watermarking" International Journal of Scientific and Research Publications, Volume 3, Issue 4, April 2013
2. C. Busch, W. Funk, and S. Wolthusen, "Digital watermarking: From concepts to real-time video applications," *IEEE Trans. Computer. Graphics Application.*, vol. 19, no. 1, pp. 25–35, Jan./Feb. 1999.
3. "DCT based video watermarking", IEEE Transactions on Consumer Electronics, Vol. 44, No. 1, February 1998
4. YANG WEN, Hui Lin WU, DEHUI YIN, JIE HE1, BINGFA LI,HAO YIN," Video digital watermark research based on MPEG4"Fourth International Conference on Image and Graphics, July 2007
5. C. I. Podilchuk and E. J. Delp, "Digital watermarking: Algorithms and applications," *IEEE Signal Process. Mag.*, vol. 18, no. 4, pp. 33–46, Jul. 2001.
6. M. A. Suhail and M. S. Obaidat, "Digital watermarking-based DCT and JPEG model," *IEEE Trans. Instrum. Meas.*, vol. 52, no. 5, pp.1640–1647, Oct. 2003.
7. Wenhai Kong1, Bian Yang1, Di Wu1, and Xiamu Niu "SVD Based Blind Video Watermarking Algorithm" First International Conference on Innovative Computing, Information and Control (ICICIC'06) © 2006 IEEE
8. JUN ZHANG' JIEGU LI' LING ZHANG, "Video Watermark Technique in Motion Vector" © 2001 IEEE
9. B. Chen and G. Wornell, "Quantization index modulation: A class of provably good methods for digital watermarking and information embedding,"*IEEE Trans. Inf. Theory*, vol. 47, no. 4, pp. 1423–1443, May 2001
10. F. Ourique, V. Kicks, R. Jordan, and F. P. Gonzalez, "Angle QIM: "A novel watermark embedding scheme robust against amplitude scaling distortions," in *Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing*, 2005, pp. 797-800.
11. Hui-Yu Huang, *Member, IEEE*, Cheng-Han Yang ,and Wen-HsingHsu, "A Video Watermarking Technique Based on Pseudo-3-D DCT and Quantization Index Modulation" *IEEE Transactions on Information Forensics and Security*, Vol.5,No. 4,December 2010.

Kumari Subhadra otta and Sushree satvatee swain are with the Department of Electronics & communication Engineering, Kalinga Institute of Industrial Technology, Bhubaneswar-751204, India (e-mail: subhadra.otta@gmail.com) (ssatvatee16@gmail.com).