Review Paper on Video Watermarking Techniques

Gopika V Mane[*], G. G. Chiddarwar[**]

[*] Department of Computer Engineering , Sinhgad College of Engineering, Pune. Maharashtra
[**] Department of Computer Engineering , Sinhgad College of Engineering, Pune. Maharashtra

Abstract- The protection and illegal redistribution of digital media has become an important issue in the digital era. This is due to the popularity and accessibility of the Internet now a days by people. This results in recording, editing and replication of multimedia contents. Digital watermarking can be used to protect digital information against illegal manipulations and distributions. Digital watermarking technique is the process of embedding noise-tolerant signal such as audio or image data in the carrier signal. This technique provides a robust solution to the problem of intellectual property rights for online contents. This paper reviews different aspects and techniques of digital watermarking for protecting digital contents.
.

Index Terms- Attacks, Content protection, Digital properties, DWT, SVD, Security, Watermarking techniques.

I. INTRODUCTION

Digital data are distributed across high-speed networks like the Internet and World Wide Web. This data is easily accessible for sharing. Due to this access possibility of tempering data and republishing it as own is increased. This leads the motivation of techniques providing security to this multimedia content. Digital watermarking is the technique used for this purpose. Various techniques of watermarking are used to insert data about ownership of contents, which help to keep the integrity of data.
A watermark is information about origin, ownership, copy control etc. This information is embedded in multimedia content with taking care imperceptibly and robustness.The watermark is embedded and extracted as per requirement. Video watermarking is different from image watermarking, because additional data are available here that allows information to be more redundantly and reliably embedded.

Digital video is a sequence or collection of consecutive still images. The amount of information that can be embedded in the video sequence is called payload. In reality video watermarking techniques need to meet other challenges than that in image watermarking schemes such as large volume of the inherently repeated sequence of data between frames.

The watermark embedding scheme can either embed the watermark into the host signal or to a transformed version of the host signal. Transform domain watermarking is a scheme that is used to transform image frequency domain in such a way to modify the transform coefficient. Some common transform domain watermarking for image data can be Discrete Cosine Transform (DCT) based [2, 3] or Discrete Wavelet Transform (DWT) based [4]. This scheme is very useful for taking advantage of perceptual criteria in the embedding process for designing watermark techniques. Spatial domain watermarking on the other hand has the capability of performing some transformation directly on image pixels. The use of perceptual models is also an important component in generating an effective and acceptable watermarking scheme for audio just as it is used in image watermarking [3, 4].

This paper is organized into five sections. The subsequent section explains the important aspects of video watermarking. Section II focuses the widespread techniques of video watermarking where various domains of video watermarking are explored and a robust algorithm in each domain is considered.

II. ASPECTS OF VIDEO WATERMARKING

Video sequencing is a collection of consecutive and equally time spaced still images. Apparently any image watermarking technique can be extended to watermark videos, but in reality video watermarking techniques needs to meet other challenges. Watermarked video sequences are very much susceptible to pirate attacks such as frame averaging, frame swapping, statistical analysis, digital-analog (AD/DA) conversion, and lossy compressions [1].

Watermarking systems can be characterized by a number of defining properties including embedding effectiveness, fidelity, data payload, blind or informed detection, false positive rate, capacity, robustness, perceptual transparency, security, cipher and watermark keys, modification and multiple watermark, cost, tamper resistance, unobtrusiveness, ready detection, unambiguous, sensitivity, and scalability. Some of them are common to more practical applications. In this section, such general properties will be listed and briefly discussed and focus will put on video watermarking. These properties are discussed due to their importance in watermarking applications.

A. Perceptual Transparency

Invisibility is the degree at which an embedded watermark remains unnoticeable when a user views the watermarked contents. However this requirement conflicts with other requirements such as tamper resistance and robustness, especially against lossy compression algorithms. To survive the next generation of compression algorithms, it will probably be necessary for a watermark to be noticeable to a trained observer which is asked to compare the original and the marked version of the video.

B. Robustness

Robustness is the resilience of an embedded watermark against removal by signal processing. The use of music, images and video signals in digital form, commonly involves many types of distortions, such as lossy compression. For watermarking to be useful, the mark should be detectable even after such distortions occurred. Robustness against signal distortion is better achieved if the watermark is placed in perceptually significant parts of the signal.

Due to large amounts of data and inherent redundancy between frames, video signals are highly vulnerable to pirate attacks, such as frame averaging, frame dropping, rotation, sharpening [1].

C. Capacity

Capacity is that amount of information that can be expressed by an embedded watermark. Depending on the application at hand, the watermarking algorithm should allow a predefined number of bits to be hidden.

III. REVIEW OF VIDEO WATERMARKING TECHNIQUES

Many digital watermarking schemes have been proposed in the literature for still images and videos. Most of them operate on uncompressed videos [8, 11, 13], while others embed watermarks directly into compressed videos [12, 13]. Video watermarking applications can be grouped as security related like Copy control [8], fingerprinting, ownership identification, authentication, tamper resistance etc. or value added applications like legacy system enhancement, database linking, video tagging, digital video broadcast monitoring [8], Media Bridge etc.

Existing video watermarking techniques are divided into different categories as shown in Figure 1. They can be divided into 3 main groups based on the domain that the watermark is embedded.

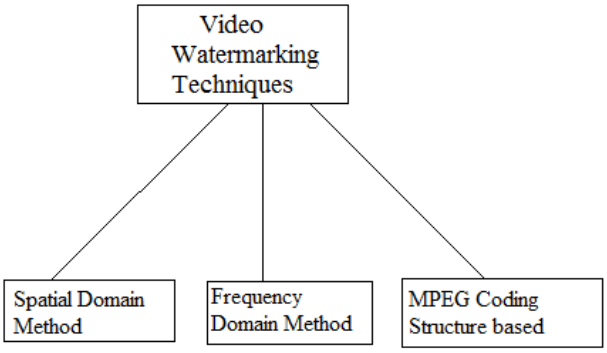

Figure 1. Classification map of existing digital video watermark techniques

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 [15]*

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 stegnography as it is a simple and powerful tool for it.But it can not 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 [14]. 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 [6-8], 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 [14]*

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 altered, then IDFT. Only the first frame of each GOP 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 [14]*

In Discrete Cosine Transform, an image is broken up into different frequency bands, to get middle frequency bands of an image where watermark can be embedded easily.

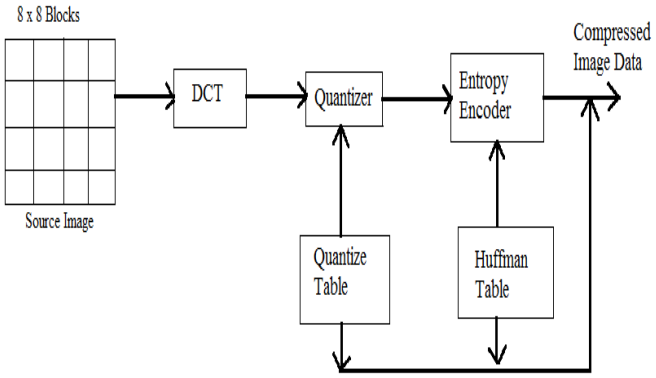

Figure 2. Process of Discrete Cosine Transform (DCT)

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

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

   $$D(i,j) = \frac{1}{\sqrt{2N}} C(i) C(j) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} p(x,y) \cos\left[\frac{(2x+1) i\pi}{2N}\right] \cos\left[\frac{(2y+1) j\pi}{2N}\right]$$

   P (x, y) is x, the element of an image represented by matrix p .N is size of block that DCT is done on. The equation calculates one entry (i, j) of the transformed image from pixel values of the original image matrix.

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.Qunatization 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 zig-zag 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.

The basic idea in the DWT for a one dimensional signal is the following. A signal is split into two parts, usually high frequencies and low frequencies. The edge components of the 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.

Let

$$H(\omega) = \sum_k h_k e^{-jk\omega};$$

And

$$G(\omega) = \sum_k h_k e^{-jk\omega};$$

be a lowpass and a highpass filter, respectively. A signal, x[n] can be decomposed recursively as

$$c_{j-1,\,k} = \sum_n h_{n-2k} c_{j,\,n}$$

$$d_{j-1,\,k} = \sum_n g_{n-2k} c_{j,\,n}$$

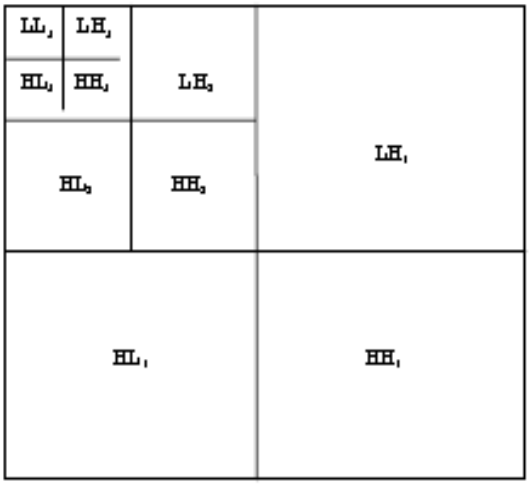

Figure 3. The model of DWT decomposition

for j = J+1, J,…., J_0 where $c_{J+1,k} = x[k]$, k Є Z, J+1 is the high resolution level index, and J_0 is the low resolution level index.

In the encoding part of DWT while watermarking, we first decompose an image into several bands with a pyramid structure as shown in Fig. 3 and then add a pseudo-random sequence (Gaussian noise) to the largest coefficients which are not located in the lowest resolution.

- *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.

Laplacian pyramid and the directional filter Bank [4] are combined in Contourlet transform. Figure 4 shows a multiscale and directional decomposition using a combination of a Laplacian pyramid (LP) and a directional filter bank (DFB) [4]. Bandpass images from the LP are fed into a DFB so that

directional information can be captured. The scheme can be iterated on the coarse image. The combined result is a double iterated filter bank structure, named contourlet filter bank, which decomposes images into directional subbands at multiple scales.

The result of the process described above returns decomposition of the input video frames with different frequency bands. A watermark is also decomposed using CT and mapped with low pass coefficients of host video frames. Inverse Contourlet Transform (ICT) is applied to the modified sub bands to get final watermarked video.

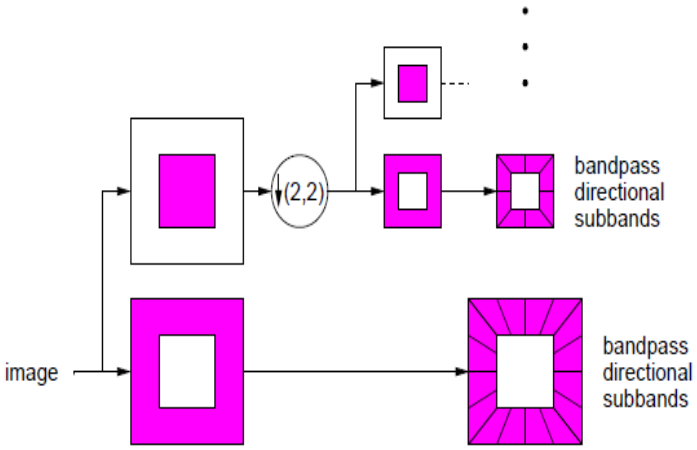

Figure 4. The contourlet filter bank

C. Watermarks Based on MPEG Coding Structures

Video watermarking techniques that use MPEG-1, -2 and -4 coding structures as primitive components are primarily motivated by the goal of integrating watermarking and compression to reduce overall real-time video processing complexity. Compression in block-based schemes like MPEG-2 is achieved by using forward and bi-directional motion prediction. There are a number of MPEG-2 and -4-based techniques that have been proposed, including approaches based on GOP modification, high frequency DCT coefficient manipulation, DCT block classification [1].

In [5], video object watermarking is based on the structure of MPEG-4. This technique can be easily added to the embedding and detection schemes without changing the watermarking algorithm. It modifies some predefined pairs of quantized DCT coefficient in the luminance block of pseudo-randomly selected MBs. It is based on spread-spectrum techniques. Dividing the image into blocks of equal size, them binary sequence is generated using a secret key, and then adds to the image.

In [6], watermarking procedure embeds copyright protection into video sequences which is object based transparent. Each watermark is created by shaping an author and video dependent pseudo-random sequence according to the perceptual masking characteristics of the video. As a result, the watermark adapts to each video to ensure invisibility and robustness. Furthermore, the noise like watermark is statistically undetectable to prevent unauthorized removal.

In [7], Mobasseri proposed direct sequence watermarking using m-frames This scheme applies a direct sequence spread spectrum model to the watermarking of the digital video. First, video signal is modeled as a sequence of bit planes arranged along the time axis. Watermarking of this sequence is a two layer operation. A controlling m-sequence first establishes a pseudorandom order in the bit plane stream for later watermarking.

D. Other Watermarking Techniques

The watermark can be either directly inserted in the raw video data or integrated during encoding process or implemented after compressing the video data. In this section we briefly discuss some of video watermarking techniques present in literature.

A novel collusion resistant (CR) video watermarking approach is proposed in [8]. This is a practical frame by frame video watermarking technique. Here a basic s × s watermark pattern is first created and this pattern is repeatedly embedded so that it is centered on a fixed number of selected points known as anchors in every video frame. The part of the video frame where the basic watermark is embedded is called the footprint [8]. Anchor points are calculated using a feature extraction algorithm. After generating these watermark frames within a given host frame, spatial masking is applied on it to ensue robustness and imperceptibility criteria. Then the scaled watermark is embedded in the host data using addition.

In Watermarking using CDMA modulation [9] one of the four least significant billions are replaced by watermark planes. The bitlanes to be replaced are selected according to a random periodic quaternary sequence. The watermark plane is generated using the 1D spread spectrum methodology.

In [10] a watermarking method using variable length code (VLC) swapping was proposed. This methodology was based on the observation that in the MPEG-2, H.26l VLC tables there are pairs of code words $(r, l) \rightarrow c_0$ and $1\ (r, l \pm 1) \rightarrow c_1$ such that $length\ (c_0) = length\ (c_1)$, $lsb\ (c_0) \neq lsb\ (c_1)$. Such level-adjacent pairs are called label-carrying VLC (lc-VLC) [10]. A covert data bit U_i is embedded into a frame by extracting eligible lc-VLC, $c_i \in \{c_0\} \cup \{c_1\}$, and swapping a codeword, if necessary such that to ensure $lsb(c_i) = U_i$. This process does not use any random key based component as a result of that this method is not robust against attacks.

A perceptual watermarking (PW) method explicitly model masking properties of the HVS and utilizes these models to analyze video sequences of frames to embed watermark in the optimal way. The five main properties of the HSV namely, frequency sensitivity, luminance sensitivity, contrast masking, edge masking and temporal masking can be exploited by video watermarking techniques [11], [12].

IV. CONCLUSION

This study discuss a number of techniques for the watermarking of digital images, also focus on the limitations and promises of each. LSB substitution does not provide robustness hence it is

not a very efficient approach for digital watermarking. LSB embedded watermarks can easily be extracted using techniques that do not visually degrade the image to the point of being noticeable. DCT domain watermarking proved to be highly challenging to JPEG compression as well as considerable amounts of random noise. The wavelet domain as well proved to be highly resistant to both compression and noise, with minimal amounts of visual degradation. The counters proposed to geometric distortion typically rely on discovering the exact rotation, or shifting used in the attack. Typically these techniques are computationally pricey, and unpredictable.

ACKNOWLEDGMENT

We are thankful to staff members and students of ME-II of Sinhgad College of Engineering, Vadgaon, Pune. Maharashtra for their support during preparation of this paper.

REFERENCES

[1] T. Jayamalar, Dr. V. Radha, "Survey on Digital Video Watermarking Techniques and Attacks on Watermarks," *International Journal of Engineering Science and Technology*, vol. 12, 6963- 6967, 2010.

[2] E. Ganic and A. M. Eskicioglu, "Secure DWT-SVD Domain Image Watermarking: Embedding Data in All Frequencies," ACM Multimedia and Security Workshop 2004.

[3] P.W. Chan and M. Lyu, "A DWT-based Digital Video Watermarking Scheme with Error Correcting Code," *Proceedings Fifth International Conference on Information and Communications Security (ICICS2003)*, Lecture Notes in Computer Science, Springer, Vol. 2836, pp. 202-213, Huhehaote City, Inner-Mongolia, China, Oct. 10-13, 2003.

[4] P.W. Chan, M.R. Lyu and R.T. Chin "*A Novel Scheme for Hybrid Digital VideoWatermarking: Approach, Evaluation and Experimentation*," submitted to IEEE Transactions on Circuits and Systems for Video Technology.

[5] B. Vassaux, P. Nguyen, S. Baudry, P. Bas, and J. Chassery, "Scrambling technique for video object watermarking resisting to mpeg-4," *Proceedings Video/Image Processing and Multimedia Communications 4th EURASIP-IEEE Region 8 International Symposium on VIPromCom*, pp. 239-244,2002

[6] M. Swanson, B. Zhu, B. Chau, and A. Tewfik, "Object- Based Transparent Video Watermarking," *Proceedings IEEE Signal Processing Society 1997 Workshop on Multimedia Signal Processing*, Princeton, New Jersey, USA, Jun.23-25, 1997.

[7] B. Mobasseri, "Direct sequence watermarking of digital video using m-frames," *Proceedings International Conference on Image Processing (ICIP-98)*, Vol. 3, pp. 399-403, Chicago, Illinois, Oct. 4-7, 1998.

[8] K. Su, D. Kundur and D. Hatzinakos, "A novel approach to collusion-resistant video watermarking", Proceedings of the SPIE, vol. 4675, pp. 491-502.

[9] B. G. Mobasseri, "Exploring CDMA for watermarking of digital video", (1999) proceedings of of the SPIE, vol. 3675, pp. 96-102.

[10] G. C. Langelaar, R. L. Lagendijk, and J. Biemond, "*Realtime labeling of MPEG-2 compressed video*," (1998) journal of visual communication and image representation, vol. 9, pp. 256-270.

[11] R. B. Wolfgang, C. I. Podilchuk and E. J. Delp, "Perceptual watermarks for digital images and video", Proceedings of the IEEE, vol. 87, pp. 1108-1126, (1999).

[12] M. M. Reid, R. J. Millar and N. D. Black, "Second-generation image coding: An overview", ACM Computing Surveys, vol. 29, pp. 3-29.

[13] F. Deguillaume, G. Csurka, J. Ruanaidh, and T. Pun, "Robust 3D DFT video watermarking," *Proceedings Electronic Imaging' 99: Security and Watermarking of Multimedia Contents*, Vol. 3657, San Jose, CA, Jan. 1999.

[14] Chris Shoemaker, "Hidden Bits: A Survey of Techniques for Digital Watermarking", Independent Study, 2002.

[15] http://www.vu.union.edu/~shoemakc/watermarking/watermarking.html

AUTHORS

First Author – GopikaV Mane completed her B.E. From Shivaji University, Kolhapur, Maharashtra. She is pursuing M.E in Computer Network from Sinhgad College of Engineering, Vadgaon, Pune. Maharashtra.
Email-id : gopikamane@gmail.com
Second Author – G. G. Chiddarwar, completed M.E from University of Pune and working as Assistant Professor in Sinhgad College of Engineering, Vadgaon, Pune. Maharashtra.
Email-id : ggchiddarwar.scoe@sinhgad.edu