

Neural Network Based Transformation Selection in Video Watermarking

Ersin Elbasi¹ and Ahmet M. Eskicioglu²

¹The Graduate Center, The City University of New York
365 Fifth Avenue, New York, NY 10016

²Department of Computer and Information Science, Brooklyn College
The City University of New York, 2900 Bedford Avenue, Brooklyn, NY 11210
eelbasi@gc.cuny.edu, eskicioglu@sci.brooklyn.cuny.edu

Abstract

Because of large amount of frames, similarity between frames and temporal attacks (frame dropping, frame averaging, frame swapping etc.), video watermarking process is more difficult than image watermarking. Current image watermarking methods cannot solve these difficulties. One of the important issue in digital video watermarking is the methodology selection. For one group of pictures, DCT might give better result; however, for some others, DWT might give better results. We propose a novel *Artificial Neural Network* (ANN) based classification system to select the best transformation method in the embedding process for the Group of Pictures (GOP). Experimental results show that transformation selection based watermarking increases the robustness against geometric attacks, and increases the quality of the watermarked video.

1 Introduction

Digital watermarking has received increasing attention in recent years. Distribution of movies, music, and images is now faster and easier via computer technology, especially on the Internet. Hence, the content owners (e.g., movie studios and recording companies) are concerned about illegal copying of their content [1]. Watermarking and cryptography are two standard multimedia security methods. However, cryptography is not an effective method because it does not provide permanent protection for the multimedia content after delivery to consumers. The contents of the documents are protected from stealing and manipulation during the delivery, but after decryption there is no protection for the documents.

The most important properties of a watermarking system are: robustness, invisibility, data capacity, and security. An embedded watermark should not introduce a significant degree of distortion in the cover multimedia element. Robustness is the resistance of the watermark against normal A/V processes or intentional attacks. Data capacity refers to the amount of data that can be embedded without affecting perceptual transparency. The security of a watermark can be defined to be the ability to thwart hostile attacks such as unauthorized removal, unauthorized embedding, and unauthorized detection. There are basically two approaches to embed a watermark: spatial domain and transform domain (e.g., DCT, DFT, or DWT) [2,3]. In the spatial domain, the watermark is embedded by modifying the pixel values in the original cover image. Transform domain watermarking is similar to spatial domain watermarking; in this case, the transform coefficients are modified. There are several criteria to classify watermarking techniques. Table 1 shows some fundamental categories.

Visible watermarks can be seen by eyes. For example, the CNN logo on the screen is a visible watermark. If someone tapes the show, the logo would still be on the screen. In invisible watermarking, the watermark is not visible at all. A watermarking technique that requires the original multimedia element to detect the watermark is called non-blind watermarking. A blind technique does not require the original multimedia element to detect the watermark. Semi-blind watermarking techniques require a seed and the watermarked multimedia element for detection. Another criteria in watermarking is the watermark type: Visual watermark and PRN sequence. The visual watermark is actually reconstructed, and its visual quality is evaluated. The PRN sequence allows the detector to statistically check the presence or absence of a watermark. A PRN sequence is generated by feeding a linear or nonlinear generator with a secret key. However, embedding a meaningful watermark is essential in some applications. This watermark could be a binary image, stamp, logo or label [1,2,3].

Criteria	Types
Type of Document	Image, Video, Audio, Text
Human Perception	Visible, Invisible
Working Domain	Spatial Domain, Frequency Domain
Watermark Type	Pseudo Random Number (PRN) sequence, Visual Watermark
Information Type	Non-Blind, Semi-Blind, Blind

Table 1: Categories of watermarking techniques

To provide the necessary properties (robustness, invisibility, data capacity, and security), we proposed a new system which make methodology decision based on the ANN classification [10]. This method provides robustness against common geometric attacks. It is difficult to guess and remove watermark after embedding.

2 Transformation Techniques

There are three main transformation based embedding techniques. DCT, DFT and DWT.

Discrete Cosine Transform (DCT): The DCT is the classic and popular domain to watermark. It breaks the image into different frequency bands. The frequency components are ordered in a sequential order (low frequency, mid frequency, and high frequency components). If most of the high frequency coefficients are zero, then they represent a smooth block. The DCT is faster, and its computational complexity is $O(n \log n)$. Embedding in the transform domain by modifying the DCT coefficients may offer many advantages, including robustness against unintentional image processing attacks like contrast adjustment, gamma correlation, filtering, blurring, etc. However, most of the DCT based approaches do not completely address the issue of geometric attacks like cropping.

Discrete Wavelet Transform (DWT): The DWT separates the image into a lower resolution image (LL), and horizontal (HL), vertical (LH) and diagonal (HH) detail components. High resolution subbands are locate edge and texture patterns in an image. The DWT is also computationally efficient and implemented by using simple filter convolution. The magnitudes of DWT coefficients are larger in the lowest bands (LL) at each level of decomposition. Embedding the watermark in the higher level subbands increases the robustness of the watermark. However, the image visual fidelity may be lost, and can be measured by the PSNR. With the DWT, the edges and texture pattern, can be easily identified in the high frequency bands like HH, LH, and HL. The large coefficients in these bands normally indicate edges in the image. Figure 1 shows two levels DWT decomposition for Lena image.

Discrete Fourier Transform (DFT): This approach first extracts the components of the image to be watermarked, computing its full frame DFT, and then taking the magnitudes of the coefficients. Embedding in DFT has some advantages. It provides rotation and translation invariance, which makes the scheme robust against geometric attacks. Figure 2 shows DFT coefficient selection in an image.

3 Algorithm Selection

Current algorithms show that transformation based (DWT, DCT, DFT) algorithms have some advantages and disadvantages in image watermarking. For example, with DWT the edges can be easily identified in the high frequency coefficients. Low frequencies are more robust when strong watermarks are embedded. The Discrete Wavelet Transform understands the HVS more closely in comparison with the DCT. Selecting the best transformation based watermarking algorithm for each group of pictures increases video visual fidelity.

The ANN have received interest over the recent few years, and successfully applied to a large range of problem domains. Each ANN produces solution for prediction, classification, etc. A neural network is a system composed of many simple processing elements operating in parallel whose function is determined by network structure, connection strengths, and the processing performed at computing elements or nodes. Neural networks, with their remarkable ability to derive meaning from complicated or imprecise data, can be used to extract patterns and detect trends that are too complex to be noticed by either humans or other computer techniques. The algorithm works as follows: It receives a number of inputs. Each input comes via connection that has a weight. Each neuron also has a single threshold value to compose the activation of the neuron. The activation signal is passed through an activation function to produce the output of the neuron. The training set of the frames will produce an adaptive network, which will classify the frame into three classes: DWT, DCT and DFT. The feature vector for each frame and the trained network is the input for the classification system [4, 5].

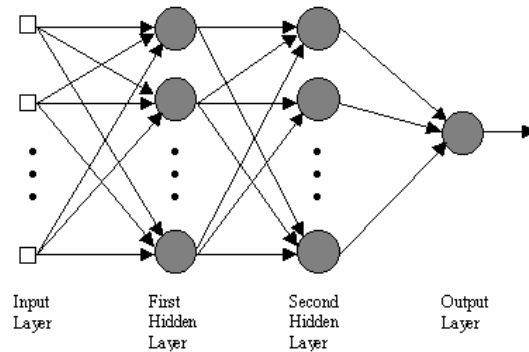


Figure 2. Structure of an ANN

Feature Extraction: Feature extraction can be defined as the operation to quantify the image quality through various parameters or functions. Main features are color, texture and edges. In this watermarking algorithm we used mainly statistical features, such as:

- a. mean
- b. variance
- c. skewness
- d. kurtosis
- e. and some edge information etc.

Network Training: In training, set of pictures have taken from 4 different video sequences. Based on the objective and subjective evaluation, for each picture is classified as DCT, DFT or DWT [4,5]. Training evaluation techniques are (in both watermarked image quality and resistant against to common attacks):

- a. Subjective Evaluation
- b. PSNR [1]
- c. M-SVD

Extracted features are trained using Backpropagation algorithm using following formulas.

$$in_i = \sum_j W_{j,i} \times a_j = W_i \times a_i \quad (1)$$

$$a_i \leftarrow g(in_i) = g\left(\sum_j W_{j,i} \times a_j\right) = g(W_i \times a_i) \quad (2)$$

Where in is the input feature vector, W is weight and g is the sigmoid function.

4 Experimental Results

Experimental results show that artificial neural network based watermarking transformation classification gives very promising results. Testing results with 80 frames taken from 4 different video sequences gives more than 90% accuracy.

Video Sequence	Accuracy (%)
1	92.3
2	88.5
3	91.2
4	94.3

5 Conclusions

The most important properties of a watermarking system are robustness, invisibility, data capacity, and security. To provide these requirements we should select best watermarking algorithm. Transformation based algorithms give different performance from image to image. We proposed a new ANN based classification system to identify best transformation algorithm in image watermarking. Results show that proposed system provides very promising results: in training %94 and in testing 91% accuracy. We will use this method in video watermarking to embed different portion of binary watermark to different sequence of frames with different transformation embedding technique in future work.

References

1. Ersin Elbasi, Ahmet M. Eskicioglu, "MPEG-1 Video Semi-Blind Watermarking Algorithm in the DWT Domain," IEEE International Symposium on Broadband Multimedia Systems and Broadcasting 2006, Las Vegas, NV, April 6-7, 2006.
2. G. Doerr, J. Dugelay, "A Guide Tour of Video Watermarking," Signal Processing: Image Communication 18 (2003), pp. 263-282.
3. C. Lin and S. Chang, "Issues and Solutions for Authenticating MPEG Video," IEEE International Conference on Acoustics, Speech and Signal Processing, 15-19 Mar 1999, pp 54-65.
4. K. Mehrotra, C. K. Mohan, S. Ranka, "Elements of Artificial Neural Network." MIT Press, pp. 70-94, 2000.
5. Shaohui L, Hongxun Y, Wen G, "Neural network based steganalysis in still images," Multimedia and Expo, 2003. ICME'03, Vol. 2 , 2003.
6. C. Hsu, J. Wu, "DCT-Based Watermarking for Video," IEEE Transaction on Consumer Electronics, Vol. 44, No. 1, February 1998, pp. 206-216.
7. H. Wang, Z. Lu, J. Pan, S. Sun, "Robust Blind Video Watermarking with Adaptive Embedding Mechanism," International Journal of Innovative Computing, Information and Control Volume 1, Number 2, June 2005.
8. Pik-Wah Chan and Michael R. Lyu, "Digital Video Watermarking with a Genetic Algorithm," Proceedings International Conference on Digital Archives Technologies Technologies (ICDAT'05), Taipei, Taiwan, June 16-17, 2005, pp. 139-153.
9. F. Hartung, B. Girod, "Digital Watermarking of Raw and Compressed Video," Digital Compression Technologies and Systems for Video Communication, pp. 205-213, October 1996.
10. Pik-Wah Chan, Michael R. Lyu and Roland T. Chin, "Copyright Protection on the Web: A Hybrid Digital Video Watermarking Scheme," Proceedings 13th International World Wide Web Conference (WWW'2004), New York , May 17-22, 2004 , pp.354-355.