Survey on Transformation Based Algorithms in Digital Image Watermarking

Ersin ELBAŞI

***Abstract*—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. Watermarking is a pattern of bits (logo or noise) inserted into a digital image, video, text or audio which identifies the copyright information [11]. This survey paper defines watermarking technique in digital images and explains main frequency based algorithms.**

***Keywords*—Watermarking, Transformation, DCT, DFT, DWT, Embedding, Detection**

I. Introduction

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. The contents of the documents are protected from stealing and manipulation during the delivery, but after decryption there is no protection for the documents [11].

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). In the spatial domain, the watermark is embedded by modifying the pixel values in the original image. Transform domain watermarking is similar to spatial domain watermarking; in this case, the coefficients are modified. Both methods have advantages and disadvantages: One disadvantage of spatial domain watermarking is that the cropping attack might remove the watermark [11].

There are several criteria to classify watermarking techniques. Table1.1 shows some fundamental categories [2].

Criteria	Types
Based on Type	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

Video watermarking is still an open research area because of a number of challenging problems: embedding large amount of data, redundancy between frames, and robustness against temporal attacks (e.g., frame averaging, frame dropping, and frame swapping) [3].

There are several application areas that range from copy protection to broadcast communication [12]. Film and music makers, TV stations, and courts are very much interested in using digital watermarking and cryptography as two complementary technologies. Table 2 shows the main application fields of multimedia watermarking.

Manuscript received October 30, 2008.
Ersin Elbaşı is with The Scientific and Technological Research Council of Turkey, Ankara (corresponding author to provide phone 312 468 5300-1124, e-mail: ersin.elbasi@tubitak.gov.tr)

Applications	Purpose
Copy Control	Prevent unauthorized copying
Broadcast Monitoring	Identify the video item being broadcasting
Fingerprinting	Trace back a malicious user
Authentication	Insure that the original content not changed
Copyright protection	Prove ownership

Table 2: Watermarking Application Areas

II. WATERMARKING METHODS

There are three major watermarking schemes in multimedia. The first is spatial domain watermarking, which basically embeds a visible logo or a PRN sequence directly to selected pixels in the host image. The second is transform domain watermarking such as DCT, DWT or DFT. The third is only for audio or video files, that is compressed domain watermarking. A video watermarking scheme usually should satisfy some requirements such as transparency, robustness, (blind) oblivious detection, free-from deadlock problem, public key detection, and so on. However, all the current watermarking methods only satisfy part of the requirements. For example, some methods are really robust (oblivious) but they are non-oblivious (not robust enough).

Cox et al. [5] proposed secure spread spectrum watermarking algorithm. This algorithm uses the Discrete Cosine Transformation in gray scale image. Proposed algorithm is as follows:

Embedding:
1.Compute the NxN DCT of an NxN gray scale cover image I.
2.Embed a sequence of real values $X=x_1,x_2,\ldots..x_n$ according to N(0,1), into the n largest magnitude DCT coefficients, excluding the DC component.
3.$V_i'=V_i(1+\alpha X_i)$, i=1,2,…,n
4.Compute the inverse DCT to obtain the watermarked cover image I'.

Detection:
1.Compute the DCT of the watermarked (and possibly attacked) cover image I*.
2.Extract the watermark X*: $X_i^*=(V_i^*-V_i)/\alpha V_i$ i=1,…n.
3.Evaluate the similarity of X* and X using.

$$Sim(X,X^*)=\frac{X.X^*}{(X^*.X^*)^{1/2}}$$

4.If Sim(X,X*) > T, a given threshold, the watermark exist.

Piva et al. [6] presented DCT based watermark recovering without resorting to the uncorrupted original image. This algorithm provides extra robustness against intentional and distortions. Proposed algorithm is as follows:

Embedding:
1.Compute NxN. DCT of the image I.
2.Reorder the DCT coefficients into zig-zag scan.
3.Generate the vector T by selecting the first L+M coefficients: $T=\{t_1,t_2,\ldots t_L,\ldots.t_{L+M}\}$.
4.Skip the lowest L coefficients and embed the watermark $X=\{x_1,x_2,\ldots,x_M\}$ in the last M numbers, to obtain $T'=\{t_1,t_2,\ldots,t_L,t'_{L+1},\ldots t'_{L+M}\}$.
5.$t'_{L+I}=t_{L+i}+\alpha.|t_{L+i}|.X_i$

Detection:
1.Apply the NxN DCT to the corrupted image I*.
2.Generate the vector T* by selecting the coefficients from (L+1)th to the (L+M)th: $T^*=\{t^*_{L+1},t^*_{L+2},\ldots t^*_{L+M}\}$
3.Compute the correlation Z between the DCT coefficients marked with a codemark X and a possibly different mark Y:

$$z=\frac{Y.T^*}{M}=\frac{1}{M}\sum_{i=1}^{M}y_i t_{L+i}^*$$

4.Compose it to the threshold

$$S_z=\frac{\alpha}{3M}\sum_{i=1}^{M}|t^*_i|$$

Experimental results demonstrated that the watermark algorithm is robust to several signal processing techniques and geometric distortions.

Dugad et al. [7] proposed wavelet based scheme for watermarking images. Algorithms is as follows:

Embedding:
1.Compute the *N*x*N* DWT of an *N*x*N* gray scale image *I*.
2.Exclude the low pass DWT coefficients.
3.Embed the watermark into the DWT coefficients > T_1: $T=\{t_i\}$, $t'_i = t_i + \alpha|t_i|x_i$, where *i* runs over all DWT coefficients > T_1.
4.Replace $T=\{t_i\}$ with $T'=\{t'_i\}$ in the DWT domain.
5.Compute the inverse DWT to obtain the watermarked image *I'*.

Detection:
1.Compute the DWT of the watermarked and possibly attacked image *I**.
2.Exclude the low pass DWT coefficients.
3.Select all the DWT coefficients higher than T_2.
4.Compute the sum $z=\frac{1}{M}\sum_{i=1}y_i t_i^*$, where *i* runs over all DWT coefficients > T_2, y_i represents either the real watermark or a fake watermark, t_i^* represents the watermarked and possibly attacked DCT coefficients.
5.Choose a predefined threshold $T_z=\frac{\alpha}{2M}\sum_{i=1}|t_i^*|$.

6.If z exceeds T_z, the conclusion is the watermark is present.

Caldelli et al. [13] proposed geometric invariant in DFT frequency domain. Algorithm works as follows:

Embedding:
1.Take the luminance layer of an YUV image.
2.Compute the Discrete Fourier Transform (DFT).
3.Select the magnitudes of some DFT coefficients according to a secret key.
4.Modify the magnitudes in such a way to create a local peak.
5.Compute the average and the standard deviation over a window centered on the point to be changed.
6.The magnitude of the center coefficient will have a value equal to the local average plus n-times (n = 4,5) the standard deviation.
7.The peaks are arranged in quadruplets, with pixels belonging to the same quadruplet being collinear.
8.Moreover these spikes are posed in such a way that quadruplets are concatenated to form a chain.
9.Concatenation is achieved by letting the final peak in each quadruplet to be the initial peak of the subsequent quadruplet of the chain.
10.The peaks form a constellation that represents the watermark and the template.
11.A very general geometric invariant (the *Cross-Ratio of four collinear points-CR*) is adopted to be resistant against complex geometrical attacks.

Detection:
1.Take the luminance layer of the watermarked YUV image.
2.Compute the Discrete Fourier Transform (DFT).
3.Identify all the local maxima through an exhaustive search.
4.If the central coefficient, within a window whose size is equal or smaller than that adopted in the embedding step, is the maximum in the window, this is assumed to be a peak.
5.The spikes located in very low and in very high frequencies are not considered.
6.The watermark is embedded in middle frequency range.
7.For an image of size 256x256 about 400 points are generally recovered.
8.This is quite a large number and the watermark is always well-hidden.
9.If an attacker wants to destroy the watermark, he should modify or delete all these coefficients, resulting in a big loss of image quality.
10.The next step is to check all the existing quadruplets of four collinear points, to compute their Cross Ratios and compare them with those characterizing the watermark.
11.If the secret key in known, it is possible to determine which are the correct values of Cross Ratios and which is the exact concatenation order among those selected.

Kusyk et al. [9] proposed a semi-blind logo watermarking for color images in the DFT domain. The proposed algorithm is as follows:

Embedding:
1.Compute the DFT of the NxN cover image.
2.Move the origin to the center.
3.Obtain the magnitudes of DFT coefficients.
4.Divide the NxN matrix of magnitudes into four (N/2)x(N/2) matrices *Mul*, *Mur*, *Mll*, *Mlr*. *ul*: upper left, *ur*:upper right, *ll*: lower left, *lr*: lower right.
5.Define three frequency bands: low, middle, and high.
6.Embed a visual binary watermark in these three bands by determining the embedding locations.
7.In each band:
a.Choose a magnitude a in matrix *Mul*, and the corresponding magnitude b in matrix *Mur*.
b.Compute the mean $m = (a+b)/2$, and choose the value of the parameter p.
c.Embedding bit 1: If $a < m-(p/2*m)$ then do not modify a and b else $a=m-(p/2*m)$ and $b=m+(p/2*m)$
d.Embedding bit 0: If $a > m+(p/2*m)$ then do not modify a and b else $a=m+(p/2*m)$ and $b=m-(p/2*m)$
8.Copy the modified magnitudes in matrix *Mul* to matrix *Mlr*.
9.Copy the modified magnitudes in matrix *Mur* to matrix *Mll*.
10.Obtain the DFT coefficients of the entire image using the modified magnitudes.
11.Compute the inverse DFT.

Detection:
1.Compute the DFT of the NxN watermarked (and possibly attacked) image.
2.Move the origin to the center.
3.Obtain the magnitudes of DFT coefficients.
4.Divide the NxN matrix of magnitudes into four (N/2) x (N/2) matrices *Mul*, *Mur*, *Mll*, *Mlr*.
5.Use the three frequency bands and the embedding locations defined in the embedding process: low, middle, and high.
6.In each band, if $a > b$ then bit = 0 else bit = 1.

Ganic et al. [10] proposed DWT-SVD based watermarking algorithm. Embedding and extraction algorithms are as follows:

Embedding:
1.Using DWT, decompose the cover image into four subbands: LL, LH, HL, and HH.
2.Apply SVD to each subband image: $A^k = U_a^k \Sigma_a^k V_a^{kT}$
3.Apply SVD to the visual watermark: $W = U_W \Sigma_W V_W^T$
4.Modify the singular values in each subband: $\lambda_i^{*k} = \lambda_i^k + \alpha_k \lambda_{wi}$, i=1,…,n

5.Construct the watermarked image: $A^{*k} = U_a^k \Sigma_a^{*k} V_a^{kT}$

Extraction:
1.Decompose the watermarked cover image into four subbands: LL, HL, LH, and HH.
2.Apply SVD to each subband image: $A^{*k} = U_a^k \Sigma_a^{*k} V_a^{kT}$
3.Extract the singular values from each subband: $\lambda_{wi}^k = (\lambda_i^{*k} - \lambda_i^k)/\alpha_k, i = 1,...,n$
4.Construct the four visual watermarks using the singular vectors: $W^k = U_W \Sigma_W^k V_W^T$

Chae et al. [14] proposed robust embedding in wavelet coefficients. Algorithm is as follows:

1.Decompose by one level the host and signature images using the DHWT. This results in four bands, which are usually referred to as the LL, LH, HL and HH bands.
2.Each signature image coefficient is expanded into 2x2 block as follow:
3.Each coefficient value is linearly scaled to a 24 bit representation.
4.Let A, B, C represent, respectively, the most significant byte, the middle byte, and the least significant byte in a 24 bit representation. Three 24- bit numbers, A',B',C', are generated with their most significant bytes set to A, B and C, respectively, and with their two least significant bytes set to zero.
5.The host image coefficients are also linearly scaled within each band to a 24 bit representation. The minimum and maximum values in each band will be used in the inverse transformation below.
6.The scaled host image coefficients are now added to the expanded signature transform to form a new fused transform. Let h(m,n) be the (m,n)th wavelet coefficient of the host image, and let s(m,n) be the (m,n)th signature coefficient after forming the expanded blocks as described in the above. Note that after expansion each of the bands in the signature wavelet transform is of the same dimension as the host image bands. The fused (m,n)th coefficient is the computed as:

$$w(m,n) = \alpha.h(m,n) + s(m,n)$$

7.Where the scale factor determines the relative percentage of the host and signature image components in the new image.
8.The fused transform coefficients in each band are scaled back to the levels of the host image transform coefficients using the minimum and maximum coefficient values in step 3.
9.An inverse transform is now computed to give the watermarked image.
10.In detection following similarity formula used:

$$S = \frac{\sum_{m,n} s^*(m,n).s(m,n)}{\sum_{m,n} (s^*(m,n))^2}$$

III. Attacks on Watermarked Image

A watermark should be robust against attacks. We can classify attacks in several ways. Direct or indirect attacks:
1. Direct attacks attempt to remove, obscure, or render the watermarks undetectable in the content.
2. Indirect attacks leave the watermark undamaged, but seek to undermine the validity of the scheme that uses the watermark as its basis.

Another attack classification scheme is based on the attack type: Geometric attacks and statistical attacks:
1. Common signal processing: The watermark should be detected after signal processing attacks such as digital-to-analog, analog-to-digital conversion, resampling, gaussian noise, histogram equalization, etc.
2. Common geometric distortions: Rotation, resizing, cropping and scaling are the most common attacks in this class.

IV. Evaluation in Watermarking

Measurement of image and video quality is a challenging problem in many applications from lossy compression to printing attacks. The quality measures can be classified into two groups: subjective and objective. There are a number of objective measures. We mention some of these measures [107].

The Mean Square Error (MSE): MSE is an old, proven measure of control and quality the MSE is defined as follows:

$$MSE = \frac{\sum (f(i,j) - F(i,j))^2}{N^2},$$

where *f (i,j)* is the original image that contains *NxN* pixels, and *F (i, j)* is the watermarked image.

The Peak-signal-to Noise Ratio (PSNR): The PSNR is most commonly used as a measure of quality of reconstruction in image watermarking. It is a ratio between the maximum value of a signal and the magnitude of background noise. It is most easily defined via the mean squared error.

$$PSNR = 20 \times \log_{10}\left(\frac{255}{RMSE}\right),$$

where RMSE is the square root of MSE.

Measure of Singular Value Decomposition (M-SVD): M-SVD is a new measure which expresses the quality of

watermarked images. It is based on the Singular Value Decomposition (SVD). M-SVD is a bivariate measure that computes the distance between the singular values of the original image and watermarked image blocks.

$$D_i = SQRT\left[\sum_{i=1}^{n}(s_i - s'_i)^2\right],$$

where s_i are the singular values of the original block, s_i are the singular values of the distorted block, and n is the block size. If the image size is k, we have (k/n) x (k/n) blocks.

The numerical measure is derived from the graphical measure. It computes the global error expressed as a single numerical value depending on the distortion type:

$$M - SVD = \frac{\sum_{i=1}^{(k/n)\times(k/n)}(|D_i - D_{mid}|)}{(k/n)\times(k/n)},$$

where D_{mid} represents the mid point of the sorted D_i's, k is the image size, and n is the block size.

Similarity Ratio (SR): Defined by SR = S/(S+D), where S denotes the number of matching pixel values in compared images, and D denotes the number of different pixel values in compared images. The Similarity Ratio is used in evaluation of non-blind watermark extraction.

V. CONCLUSION

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. 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 most important properties of a watermarking system:

- Robustness
- Invisibility
- Data capacity
- Security

There are several issues in video watermarking that makes processing difficult. Such as:

- Large amount of frames
- Similarity between frames
- Temporal attacks (frame dropping, frame averaging, frame swapping etc.)

REFERENCES

[1] E. Elbasi, A. M. Eskicioglu, "A DWT-Based Robust Semi-Blind Image Watermarking Algorithm Using Two Bands", IS&T/SPIE's 18th Annual Symposium on Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents VIII Conference, San Jose, CA, January 15–19, 2006.

[2] P. Tao and A. M. Eskicioglu, "A Robust Multiple Watermarking Scheme in the DWT Domain," Optics East 2004 Symposium, Internet Multimedia Management Systems V Conference, Philadelphia, PA, October 25-28, 2004, pp. 133-144.

[3] P. Chan, M. R. Lyu and R. T. Chin, "Copyright Protection on the Web: A Hybrid Digital Video Watermarking Scheme," Proceedings 13th International World Wide Web Conference, New York, May 17-22, 2004, pp.354-355.

[4] C. Hsu, J. Wu, "DCT-Based Watermarking for Video", IEEE Transaction on Consumer Electronics, Vol. 44, No. 1, February 1998, pp. 206-216

[5] I. J. Cox, J. Kilian, T. Leighton and T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia," IEEE Transactions on Image Processing, 6(12), December 1997, pp.1673-1687.

[6] A. Piva, M. Barni, F. Bartolini, V. Cappellini, "DCT-based Watermark Recovering without Resorting to the Uncorrupted Original Image," Proceedings of International Conference on Image Processing, Washington, DC, October 26 - 29, 1997, pp. 26-29.

[7] R. Dugad, K. Ratakonda and N. Ahuja, "A New Wavelet-Based Scheme for Watermarking Images," Proceedings of 1998 International Conference on Image Processing (ICIP 1998), Vol. 2, Chicago, IL, October 4-7, 1998, pp. 419-423.

[8] W. Zhu, Z. Xiong and Y.-Q. Zhang, "Multiresolution Watermarking for Images and Video," IEEE Transactions on Circuits and Systems for Video Technology, 9(4), June 1999, pp. 545-550.

[9] J. Kusyk and A. M. Eskicioglu, "A Semi-blind Logo Watermarking Scheme for Color Images by Comparison and Modification by Comparison and Modification of DFT Coefficients Optics East 2005, Multimedia Systems and Applications VIII Conference, Boston, MA, October 23-26, 2005.

[10] E.Ganic, A.M. Eskicioglu, "Robust DWT-SVD domain image watermarking: embedding data in all frequencies", International Multimedia Conference, Proceedings of the 2004 workshop on Multimedia and security table of contents, Magdeburg, Germany.

[11] Ersin Elbasi, "Multimedia Security: Digital Image and Video Watermarking", Doctorate Thesis, 2007, The City University of New York.

[12] G. Doerr, J. Dugelay, "A Guide Tour of Video Watermarking", Signal Processing: Image Communication 18 (2003), pp. 263-282.

[13] R. Caldelli, M. Barni, F. Bartolini, A. Piva: Geometric-Invariant Robust Watermarking through Constellation Matching in the Frequency Domain. ICIP 2000.

[14] J. J. Chae, B. S. Manjunath, "A Robust Embedded Data from Wavelet Coefficients", SPIE International Conference on Storage and Retrieval for Image and Video Databases VI,1998.