A ROBUST OBLIVIOUS WATERMARKING SCHEME

Mahalingam Ramkumar and Ali N. Akansu

Department of Electrical and Computer Engineering
New Jersey Institute of Technology
New Jersey Center for Multimedia Research
University Heights, Newark, NJ 07102

ABSTRACT

In this paper, a robust watermarking scheme for images is proposed. The proposed method can be also be easily extended to other signals like audio and video. In the proposed method an optimal solution is obtained for maximizing the detection statistic (which is an indication of the degree of certainty with which the signature or the watermark is detected), for a given permitted distortion of the host signal, and additive noise variance. Other issues for improving the security of the watermarking scheme, like key based transforms, are also addressed.

1. INTRODUCTION

Establishing ownership of creations like books or blueprints, have traditionally been done by obtaining copyright on that content, perhaps from the copyright office. However, the nature of digital content makes traditional copyright mechanisms unsuitable for establishing ownership [1]. Digital watermarking [2] is a means of protecting multimedia content from intellectual piracy. It is achieved by imperceptibly modifying the original content to insert a "signature". The signature is extracted when necessary to show proof of ownership. In this paper, we present a robust watermarking scheme for images. The proposed scheme is also applicable for video and audio signals, with very little modifications.

Let I be the original (cover) image. A watermark embedding function $\mathcal{E}$ inserts a watermark S in the image I to generate the watermarked image $\hat{I} = \mathcal{E}(I, S)$. The existence of the watermark S in an image $\tilde{I}$ is checked by a detector function $\mathcal{D}$. Watermark detectors can be broadly classified into two categories. *Non oblivious* detectors need the original image I to check for the presence of the signature S in $\tilde{I}$. On the other hand, *oblivious* detectors [3, 4] *do not* require the original image. We shall term the output of the detector,

$$s_d = \begin{cases} \mathcal{D}(\tilde{I}, S, I) & \text{non oblivious detector} \\ \mathcal{D}(\tilde{I}, S) & \text{oblivious detector} \end{cases} \quad (1)$$

as the *detection statistic*. The detection statistic is an indication of the *degree of certainty* with which the signature S is detected in the image $\tilde{I}$.

2. DETECTION STATISTIC

Typically, the signature S takes the form of a Gaussian or binary pseudo random sequence $\mathbf{s}$ (say of length N) generated from a *key* $\mathcal{K}$. The watermark embedding and detection operations can therefore be written as

$$\hat{I} = \mathcal{E}(I, \mathbf{s}) \quad \tilde{\mathbf{s}} = \mathcal{D}(\tilde{I}, < I >) \quad s_d = \frac{\mathbf{s}^T \tilde{\mathbf{s}}}{|\mathbf{s}||\tilde{\mathbf{s}}|} \quad (2)$$

In other words, the detection statistic ($-1 \leq s_d \leq 1$) is a measure of (normalized) *inner product*, or normalized correlation of the embedded and the detected signature sequences.

The normalized inner product of randomly generated signature sequences will also be random. More specifically, for large N, the distribution of the inner product will be Gaussian. Let x_i and y_i, $i = 1, \ldots, N$ be i.i.d. of variance $\sigma_x^2 = \sigma_y^2 = \frac{1}{N}$, and let $q_i = x_i y_i$. The inner-product $p = \sum_{i=1}^{N} q_i = \sum_{i=1}^{N} x_i y_i$. Since x_is and y_is are independent, the variance of q_i, is given by

$$\sigma_q^2 = \sigma_x^2 \times \sigma_y^2 = \frac{1}{N} \times \frac{1}{N} = \frac{1}{N^2}. \quad (3)$$

Therefore, for large N, from central limit theorem (CLT), $p \sim \mathcal{N}[0, \frac{1}{N}]$.

If the creator (or the pirate) has *absolutely no freedom* in choosing the signature, and if the detection statistic s_d obtained is say 6 times the standard deviation (if $s_d = 6\frac{1}{\sqrt{N}}$), then we could say that the signature is detected with a probability of error (or probability of false alarm) of less than $Q(6) \approx 1 \times 10^{-9}$, where $Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty \mathrm{e}^{\frac{t^2}{2}} \mathrm{dt}$. In other words, on an average, only 1 out of 1×10^9 signatures chosen randomly can yield such a high correlation.

3. WATERMARKING ALGORITHMS

Usually, the watermark is inserted in some transform domain. Let $\mathbf{C} = \mathcal{T}(I)$, where $\mathcal{T}$ denotes some transform and $\mathbf{C}$ are the transform coefficients of I. The transform coefficients may also be of significantly reduced degrees of freedom (for achieving invariance to possibly scale, translation, rotation, cropping etc.) Further, only a subset $\mathbf{c} \in \Re^N$ of $\mathbf{C}$ may be modified to embed the watermark. Let $\mathbf{C} = \mathbf{c} \cup \bar{\mathbf{c}}$, where $\mathbf{c} \cap \bar{\mathbf{c}} = \Phi$. The coefficients $\bar{\mathbf{c}}$ are unaffected by the watermarking process. The overall embedding operation may be expressed as

$$\mathbf{C} = \mathcal{T}(I) \quad \hat{\mathbf{c}} = \mathcal{E}(\mathbf{c}, \mathbf{s}) \quad \hat{\mathbf{C}} = \hat{\mathbf{c}} \cup \bar{\mathbf{c}} \quad \hat{I} = \mathcal{T}^{-1}(\hat{\mathbf{C}}) \quad (4)$$

Let $\tilde{I} = \hat{I} + \mathbf{N}$ be the image in which the presence of the watermark is tested. The detection operation can be expressed as

$$\tilde{\mathbf{C}} = \mathcal{T}(\tilde{I}) \quad \tilde{\mathbf{s}} = \mathcal{D}(\tilde{\mathbf{c}}) \quad s_d = \frac{\mathbf{s}^T \tilde{\mathbf{s}}}{|\mathbf{s}||\tilde{\mathbf{s}}|} \quad (5)$$

The watermarking algorithms that fit into the general model of Eq. (4 - 5) can further be classified into 3 types, (Type I, Type II and Type III) depending on the embedding and detection operators $(\mathcal{E}, \mathcal{D})$.

0-7803-6297-7/00/$10.00 © 2000 IEEE

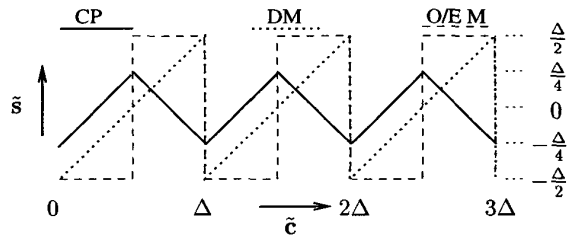

Fig. 1. Some periodic functions $\tilde{\mathbf{s}} = \mathcal{D}(\tilde{\mathbf{c}})$ for Continuous Periodic (CP) SNS, Dither Modulation (DM), and Odd /Even Modulation (O/E M)

3.1. Type I

For Type I methods, $(\mathcal{E}, \mathcal{D})$, take the form of linear addition. Mathematically, $\hat{\mathbf{c}} = \mathbf{c} + \mathbf{s}$. Type I methods can further be classified as non oblivious methods, where $\mathcal{D}(\tilde{\mathbf{c}}) \equiv \tilde{\mathbf{c}} - \mathbf{c}$ (for example, the method in [2]), and oblivious methods (for example, [3]), where $\mathcal{D}(\tilde{\mathbf{c}}) \equiv \tilde{\mathbf{c}}$ (no operation).

3.2. Type II

Type II methods generally have a non-linear element in the embedding and detection operators. In most Type II methods the non-linear operation takes the form of quantization [5, 6, 7]. The purpose of the non-linear operation is to achieve suppression of self-noise (for oblivious detection methods, $\mathbf{c}$ is noise). Ref. [8] generalized the concept of Type II methods. The generalization was based on the fact that it was the periodic nature of quantization process that is responsible for self-noise suppression. Most proposed Type II methods force the coefficients to quantize to odd or even values. This is equivalent to using the square wave periodic function (O/E M) in Figure 1. Chen *et. al* [7] proposed a dither modulation (DM) technique which is equivalent to using the saw-tooth wave in Figure 1. In Refs. [8, 9], we proposed two continuous periodic functions - CP (triangular wave) and CsP (cosine). It was also shown that continuous periodic functions outperform quantizer functions for purposes of self-noise suppression.

Ref. [8] viewed data hiding as a *sophisticated signaling scheme*, where the origin of the signal constellation has to be *estimated* at the receiver. The over-all data hiding method utilizes a *floating signal constellation*[10]. The floating signal constellation consists of a signal constellation with *known origin*, which is translated in space by an embedding function $\mathcal{E}$, to a point close to the location of the original content (image) so that the distortion introduced in the image is minimal. At the receiver a detector function $\mathcal{D}$, employing the same periodic function as $\mathcal{E}$, maps back the received image to a point in the constellation with known origin.

3.3. Type III

A disadvantage of conventional Type II data hiding methods is that the period of the quantizer, Δ, (or of the periodic function used) determines the distortion introduced. In other words, the robustness needed is not given any consideration for choice of Δ.

Ref. [8] also proposed a further extension of Type II systems, (Type III systems) which introduced *thresholding* to the distortion introduced by Type II systems. While the distortion introduced in Type II systems is generally uniformly distributed between $\pm\frac{\Delta}{2}$, the distortion introduced in Type III systems is thresholded to some $\pm\frac{\beta}{2}$, where, $\beta < \Delta$. Thus it is possible to choose larger values of Δ in Type III systems by decreasing β proportionally. The paper also discussed optimal choice of β and Δ depending on the *additive noise in the channel* and the *permitted distortion of the host signal.* The method for obtaining optimal Δ and β is outlined in the next section (for a more thorough treatment, see Ref. [11]).

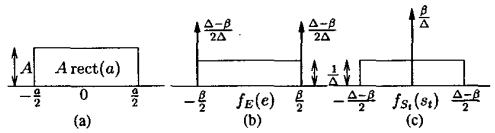

Fig. 2. (a) The rectangular function. (b) Probability distribution of distortion introduced due to data hiding and (c) distribution of noise introduced due to thresholding

The watermarking scheme outlined in this paper uses the (triangular) continuous periodic function. The embedding operation $\mathcal{E}$, characterized by a period Δ and threshold β is as follows:

$$
\begin{aligned}
p(k) &= \mathcal{D}(c(k)) \quad e(k) = s(k) - p(k) \\
e(k) &= (|e(k)| > \frac{\beta}{2}) \ ? \ \text{sign}(e(k))\frac{\beta}{2} \ : \ e(k) \\
e(k) &= (\text{rem}\left(\frac{c(k)}{\Delta}\right) > \frac{\Delta}{2}) \ ? \ -e(k) \ : \ e(k) \\
\hat{c}(k) &= (c(k) \geq 0) \ ? \ c(k) + e(k) \ : \ c(k) - e(k)
\end{aligned}
$$

In the above equation x = (Condition) ? a : b stands for "if Condition is true $x = a$ else $x = b$". The algorithm for $\mathcal{D}(\tilde{\mathbf{c}})$ is as follows:

$$
\begin{aligned}
q(k) &= \text{rem}(\frac{|\tilde{c}(k)|}{\Delta}), \quad k = 1 \cdots N \\
\tilde{s}(k) &= (q(k) \geq \frac{\Delta}{2}) \ ? \ (\frac{3\Delta}{4} - q(k)) \ : \ (q(k) - \frac{\Delta}{4})
\end{aligned} \tag{6}
$$

It is interesting to note that Type III systems are a generalization of both Type I and Type II systems. As $\Delta \to \beta$, Type III systems become Type II systems. On the other hand, as $\Delta \to \infty$, Type III systems become Type I.

3.4. Optimal Choice of Δ and β

The distortion $\mathbf{e}$ introduced by the embedding function $\mathcal{E}$ has a probability distribution and variance given by

$$
\begin{aligned}
f_E(e) &= \frac{1}{\Delta}\text{rect}(\beta) + \frac{\Delta - \beta}{2\Delta}\left[\delta(e - \frac{\beta}{2}) + \delta(e + \frac{\beta}{2})\right] \\
\sigma_e^2 &= \frac{\beta^2}{12\Delta}(3\Delta - 2\beta)
\end{aligned} \tag{7}
$$

The thresholding operation in the embedding stage introduces an additional noise $\mathbf{s}_t = \mathbf{s} - \mathcal{D}(\hat{\mathbf{c}})$ for the purpose of detection of the signature. The thresholding noise has a probability distribution and variance given by

$$
\begin{aligned}
f_{S_t}(s_t) &= \frac{\beta}{\Delta}\delta(s_t) + \frac{1}{\Delta}\text{rect}(\Delta - \beta) \\
\sigma_{s_t}^2 &= \frac{(\Delta - \beta)^3}{12\Delta}
\end{aligned} \tag{8}
$$

The pictorial representations of the probability distributions are shown in Figure 2. If the additive noise in the channel (which may consist of intentional and unintentional attacks to remove the watermark) is Gaussian with variance σ_ν^2, the probability distribution $f_Z(z)$ of the total noise $\mathbf{z} = \nu + \mathbf{s}_t$, is obtained as

Table 1. Optimal values of $k = \frac{\Delta}{\Delta_0}$ for different SNRs (SNR $= 10\log_{10}(\frac{\gamma^2}{\sigma_\nu^2})$)

SNR	k	SNR	k	SNR	k
0.00	1.87	-3.01	2.57	-4.77	3.14
-6.02	3.59	-6.99	4.04	-7.78	4.40
-8.45	4.78	-9.03	5.11	-9.54	5.41
-10.00	5.71	-13.01	8.10	-14.77	9.95

$$f_Z(z) = \int_{-\infty}^{\infty} f_\nu(x) f_{S_t}(z-x)\mathrm{d}x = \frac{\beta}{\Delta\sqrt{2\pi\sigma_\nu^2}} \mathrm{e}^{\frac{-z^2}{2\sigma_\nu^2}} + \frac{1}{2\Delta}\left\{\mathrm{erf}\left(\frac{z+\frac{\Delta-\beta}{2}}{\sqrt{2}\sigma_\nu}\right) - \mathrm{erf}\left(\frac{z-\frac{\Delta-\beta}{2}}{\sqrt{2}\sigma_\nu}\right)\right\}$$

where erf(.) denotes the *Gaussian error function*,

$$\mathrm{erf}(t) = \frac{2}{\pi}\int_0^t \mathrm{e}^{\frac{-y^2}{2}}\mathrm{d}y. \tag{9}$$

The optimal choice of Δ and β for a given permitted distortion γ^2 is obtained by maximizing the expected value of the normalized correlation given by [8, 11]

$$\rho = \frac{2\sum_{i=0}^{\infty}\int_{\frac{i\Delta}{2}}^{\frac{(i+1)\Delta}{2}}(-1)^i(\frac{(2i+1)\Delta}{4} - z)f_Z(z)\mathrm{d}z}{\sqrt{2\sum_{i=0}^{\infty}\int_{\frac{i\Delta}{2}}^{\frac{(i+1)\Delta}{2}}(\frac{(2i+1)\Delta}{4} - z)^2 f_Z(z)\mathrm{d}z}} \tag{10}$$

subject to the condition $\gamma^2 = \frac{\beta^2}{12\Delta}(3\Delta - 2\beta)$. Table 1 shows the optimal values of $k = \frac{\Delta}{\Delta_0}$, where $\Delta_0^2 = 12\gamma^2$, for different signal to noise ratios (SNR=$10\log_{10}\left(\frac{\gamma^2}{\sigma_\nu^2}\right)$). As an example, if one-eighth of the coefficients of some unitary transform of the image are used for watermarking, and if the permitted distortion of the image after addition of the watermark is restricted to have a peak SNR of 42 dB, then $\gamma^2 \approx 33$, implying $\Delta_0 \approx 20$. The expected attacks (σ_ν^2) is typically expected to be much larger than γ^2. A reasonable choice for operating at SNR of -9 dB, may be $k \approx 5$ (or $\Delta = 100$) and $\beta = 12$. As the decoder does not need to know the value of β, the value of β may be chosen depending on the nature of the image. Small values of β may be chosen for very smooth images, and larger values for highly textured images. A better approach might be to choose a high value of β and obtain the watermarked image $\hat{I}_1$. The distortion introduced due to watermarking, viz. $\hat{I}_1 - I$ may then be thresholded using a reasonable visual threshold model to obtain the final watermarked image $\hat{I}$.

4. PROPOSED WATERMARKING SCHEME

This section outlines a possible watermarking scheme for images (except for the choice of the decomposition employed, and the choice of coefficients to be modified for inserting the watermark, the proposed method is equally applicable for audio signals). The block diagram of the scheme (embedding and detection) is shown in Figure 3.

In Figure 3 I represents the cover image after equalizing the histogram by the fixed equalizer. Perhaps, high GTC (Transform Coding Gain) transforms like DCT or wavelet transforms are the best suited for watermarking applications. As high GTC transforms provide the most compact representation of the image, attacking DCT / wavelet coefficients for the purpose of watermark removal will most likely destroy the image. We use the 10-tap Daubechies filter for this purpose. Only the LL frequency subband coefficients (one fourth of the total number of coefficients) are used for watermarking purposes. The embedding and detection operators are Type III described by Eqs. (6) and (7).

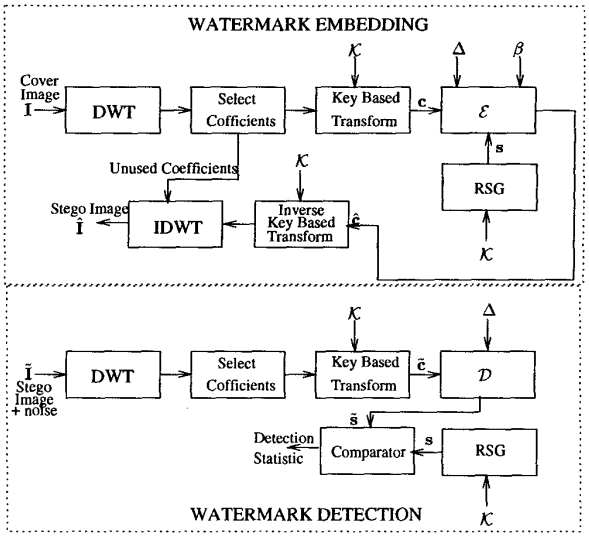

Fig. 3. Block Diagram of the Watermark Embedding and Detection

The Type II and Type III systems however, perform best for *binary* signature sequences. Therefore if the transform employed (and Δ) is known it is very easy for a pirate to remove the signature completely without introducing significant distortion in the image. A truly secure watermarking scheme, should be difficult to crack even if every step of the algorithm is public. In this case, the only 'secret' should be the key $\mathcal{K}$ (which is derived from the original image using the hash function). The security can be vastly improved by using a key based transform [12] before data embedding (and therefore before detection). In the proposed scheme, we use a simple key-based transform using cyclic all-pass filters as basis vectors [4]. Let $\mathbf{h} \in \Re^N$ and $\mathbf{H} = \mathcal{F}(\mathbf{h})$ where, $\mathcal{F}(.)$ stands for the Discrete Fourier Transform (DFT). Further, let $\mathbf{h}$ be such that $\mid H(n) \mid = 1$ for $n = 0, 1, \ldots, N-1$. Hence $(\mathbf{H}.\mathbf{H}^*) = [1, 1, \ldots, 1]$, or, $\mathcal{F}^{-1}(\mathbf{H}.\mathbf{H}^*) = [1, 0, 0, \ldots, 0]$. As $\mathcal{F}^{-1}(\mathbf{H}.\mathbf{H}^*)$ is the *circular autocorrelation* of the vector $\mathbf{h}$, it follows that all circular shifts of $\mathbf{h}$ are mutually orthogonal, and *form a basis* for $\Re^N$. As the phases ϕ_n, $n = 0, 1, \ldots, N-1$ of the elements of $\mathbf{H}$ can be arbitrary, we have N degrees of freedom for choice of the vector $\mathbf{h}$ with mutually orthogonal circular shifts. For real $\mathbf{h}$ we have $\frac{N}{2} - 1$ phase values which can be arbitrarily chosen. Thus a pseudo-random all pass sequence of length N can be generated from a pseudo-random (uniformly distributed between π and $-\pi$) sequence of length $\frac{N}{2} - 1$. The pseudo random sequence, would be generated from the key $\mathcal{K}$. If

$$\begin{aligned} \phi_k &= \begin{cases} 0 \text{ or } \pi & k = 0, k = \frac{N}{2} \\ \theta_k & k = 0 \cdots \frac{N}{2} - 1 \\ -\theta_{N-k} & k = \frac{N}{2} + 1 \cdots N - 1 \end{cases} \\ H(k) &= \cos(\phi_k) + \mathrm{i}\sin(\phi_k), k = 0 \cdots N-1, \end{aligned} \tag{11}$$

where $\theta_k, k = 1 \cdots \frac{N}{2} - 1$ are randomly distributed between π and

$-\pi$, i $= \sqrt{-1}$, then $\mathbf{h} = \mathcal{F}^{-1}(\mathbf{H})$, is a cyclic all-pass sequence. A transform employing the $\mathbf{h}$ and all its cyclic shifts as its basis can be easily implemented by cyclic correlation. If $\mathbf{x} \in \Re^N$ is a vector of coefficients, and $\mathbf{X} \in \Re^N$ are the corresponding transform coefficients,

$$\mathbf{X} = \mathcal{F}^{-1}(\mathcal{F}(\mathbf{x}).\mathcal{F}(\mathbf{h})) \quad \mathbf{x} = \mathcal{F}^{-1}(\mathcal{F}(\mathbf{X}).\mathcal{F}(\mathbf{h})^*) \qquad (12)$$

The over-all embedding operation is then as follows. The original image (after histogram equalization) undergoes DCT / Wavelet transform, and selected low to medium frequency bands are utilized for data hiding. The selected coefficients are transformed by the key based transform to obtain the coefficients $\mathbf{c}$ to be used for data embedding. The signature sequence $\mathbf{s}$ to be embedded in $\mathbf{c}$ may be obtained as a pseudo-random binary sequence using the prescribed random sequence generator (RSG) trigerred by the key $\mathcal{K}$ (which in turn is derived from hashing the original image). The coefficients obtained after embedding, viz. $\hat{\mathbf{c}}$ then undergo the inverse Key-based transform to obtain the modified DCT / wavelet coefficients, which together with the unmodified coefficients are inverted to obtain the watermarked image or the stego-image.

For detection, the received image undergoes fixed algorithms for aligning geometric features and rescaling of pixel values / histogram equalization, resulting in image $\tilde{I}$. The transformation $\mathcal{T}$ is performed on the received noisy image $\tilde{\mathbf{I}}$ to get the corresponding coefficients $\tilde{\mathbf{c}}$. The detector function $\mathcal{D}$ extracts the noisy signature sequence $\tilde{\mathbf{s}}$, which along with the signature sequence $\mathbf{s}$ (obtained from I) is input to the comparator block. The comparator obtains s_d as the normalized correlation of $\mathbf{s}$ and $\tilde{\mathbf{s}}$.

5. RESULTS AND CONCLUSIONS

The performance of the proposed watermarking scheme (in terms of the $s_d\sqrt{N}$, where false alarm probability is $P_e = Q(s_d\sqrt{N})$) for many 256 × 256 8-bpp test images, subject various attacks like JPEG compression (quality factor 15 %), SPIHT compression (0.15 bpp), resizing, and StirMark [13] is depicted in Table 2. Resizing was performed using ImageMagick. 256 × 256 images were resized to 123 × 145, saved, and then the resized images again resized to the original size of 256 × 256. StirMarked images were "re-registered" to obtain synchronization. The unwarping method used is based on iterative partitioning and matching of "feature" points, presented in Ref. [14].

Though we have used subband transforms for the proposed watermarking scheme to obtain the coefficients $\mathbf{c}$, the proposed method is equally applicable if $\mathbf{c}$ is obtained by other methods. For example, $\mathbf{c}$ may represent only the DFT magnitudes, in which case they will be invariant to (cyclic) translation of images (this however, reduces the degrees of freedom, N, by a factor of 2). By further reducing degrees of freedom, invariance to other operations may be obtained. As a simple example, for robustness to cropping, the signature may be repeated in many blocks of the image. However, reduction in degrees of freedom (N) would imply that the detection statistic should be *higher* for the same probability of false alarm, as $P_e = Q(s_d\sqrt{N})$.

Table 2. Performance of the Proposed Scheme. For example, $s_d\sqrt{N} = 10$ implies $P_e = Q(10) \approx 7.6196 \times 10^{-24}$.

Image	JPEG	SPIHT	StirMark	Resizing
Girl	10.2	9.1	15.0	11.2
Baboon	20.4	8.3	23.6	12.6
Barbara	14.3	7.9	21.3	10.7
Lena	12.1	10.4	18.5	14.8

6. REFERENCES

[1] M.Ramkumar, A.N. Akansu, "A Robust Protocol for Proving Ownership of Images", Proceedings of IEEE ITCC, pp 22-27, Las Vegas, NV, March 2000.

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

[3] W.Zeng, B. Liu, "On Resolving Rightful Ownerships of Digital Images by Invisible Watermarks", IEEE Conference on Image Processing, Vol **1** pp 552-555, Santa Barbara, CA, October 1997.

[4] M.Ramkumar, A.N. Akansu, "A Robust Scheme for Oblivious Detection of Watermarks/ Data Hiding in Still Images", *SPIE Multimedia Systems and Applications, Boston*, MA, vol **3528**, pp 474 - 481, November 1998.

[5] M.Wu, B. Liu, "Watermarking for Image Authentication", Proceedings of IEEE International Conference on Image Processing, October 4-7, 1998, Chicago, Illinois, USA, vol. **2**, pp 437 - 441.

[6] H. Inoue, A. Miyazaki, A. Yamamoto, T. Katsura, "A Digital Watermark Based on the Wavelet Transform and its Robustness on Image Compression", *IEEE International Conference on Image Processing*, Chicago, Illinois, vol **3**, pp 391-395, October 1998.

[7] B. Chen, G.W. Wornell, "Digital Watermarking and Information Embedding Using Dither Modulation", IEEE Workshop on Multimedia Signal Processing, Los Angeles, California, pp 273-278, December 1998.

[8] M.Ramkumar, A.N. Akansu, "Self-Noise Suppression Schemes for Multimedia Steganography", SPIE, International Workshop on Voice, Video and Data Communication, Multimedia Applications, Boston, vol. **3845**, September 1999.

[9] M.Ramkumar A.N. Akansu, A.A Alatan, " A Robust Data Hiding Scheme for Digital Images Using DFT", *IEEE International Conference on Image Processing*, **II**, pp 211-215, October 1999.

[10] M.Ramkumar A.N. Akansu, "Floating Signal Constellations for Multimedia Steganography," to be presented at the IEEE International Conference on Communications, New Orleans, LA, June 2000.

[11] M. Ramkumar, A.N. Akansu, "Signaling for Multimedia Steganography", submitted to the *IEEE Transactions on Signal Processing*, November 1999.

[12] M.Ramkumar, A.N Akansu, "On the Design of Robust Data Hiding Systems", 33rd *ASILOMAR Conference on Signals, Systems and Computers*, Pacific Grove, CA, October 1999.

[13] M. Kutter and F. A. P. Petitcolas. "A Fair Benchmark for Image Watermarking Systems", *Electronic Imaging: Security and Watermarking of Multimedia Contents*, vol. **3657**, pp. 226-239, San Jose, CA, USA, January 1999.

[14] I.B. Ozer, M. Ramkumar and A.N. Akansu, "A New Method for Detection of Watermarks in Geometrically Distorted Images", submitted to IEEE International Conference on Acoustics, Speech and Signal Processing", Istanbul, Turkey, June 2000.