ARES project
CONSOLIDER-INGENIO 2010 CSD2007-00004
Workpackage 3 - Task 6 (WP3.T6)
Evaluation of marking techniques in the literature
Deliverable Report

David Megías, Carmen Ruiz Vicente,
Jordi Serra-Ruiz, Mehdi Fallahpour

Universitat Oberta de Catalunya,
Estudis d'Informàtica, Multimèdia i Telecomunicació,
Rambla del Poblenou, 156, 08018 Barcelona, Spain
e-mail {dmegias,cruizvic,jserrai,mfallahpour}@uoc.edu

November 29, 2012

Contents

Abstract

This report introduces the state of the art of watermarking techniques investigated within the ARES project. The reported is divided into four chapters that focus on audio (Chapter 1), speech (Chapter 2), images (Chapter 3) and remote sensing images (Chapter 4). Each chapter gives an overview of the literature and presents the improvements developed within the ARES project.

Chapter 1

Watermarking of audio contents

This chapter presents the evaluation of the related work in the audio watermarking field. The structure of the chapter is as follows:

- Section 1.1 summarizes the work performed in the following article:

  [1] D. Megías, J. Serra-Ruiz, and M. Fallahpour, "Efficient self-synchronised blind audio watermarking system based on time domain and FFT amplitude modification," *Signal Process.*, vol. 90, pp. 3078–3092, Dec. 2010.

- Section 1.2 summarizes the work performed in the following articles:

  [2] M. Fallahpour and D. Megías, "DWT-based high capacity audio watermarking," *IEICE Transactions*, vol. 93-A, no. 1, pp. 331–335, 2010.

  [3] M. Fallahpour and D. Megías, "High capacity audio watermarking using the high frequency band of the wavelet domain," *Multimedia Tools Appl.*, vol. 52, pp. 485–498, Apr. 2011.

- Section 1.3 summarizes the work performed in the following articles:

  [4] M. Fallahpour and D. Megías, "High capacity method for real-time audio data hiding using the FFT transform," *Advances in Information Security and Its Applications*, vol. 36, pp. 91–97, 2009.

  [5] M. Fallahpour and D. Megías, "Robust high-capacity audio watermarking based on FFT amplitude modification," *IEICE Transactions*, vol. 93-D, no. 1, pp. 87–93, 2010.

[6] M. Fallahpour and D. Megías, "High capacity FFT-based audio watermarking," in *Proceedings of the 12th IFIP TC 6/TC 11 international conference on Communications and multimedia security*, CMS'11, (Berlin, Heidelberg), pp. 235–237, Springer-Verlag, 2011.

- Finally, Section 1.4 summarizes the work performed in the following article:

[7] M. Fallahpour and D. Megías, "High capacity logarithmic audio watermarking based on the human auditory system," in *Proceedings IEEE International Symposium on Multimedia*, ISM2012, 2012.

1.1 Efficient self-synchronised blind audio watermarking system

Some remarkable audio watermarking results presented in [8, 9, 10, 11] provide good results in terms of robustness and transparency, but they do not include an explicit synchronisation method. On the other hand, other audio watermarking schemes divide the cover object into several blocks such that part of the watermark is embedded into each of them. One of the key issues in these block-oriented watermarking schemes is to preserve the synchronisation, i.e. to recover the exact position of each block in the mark recovery process. Many audio watermarking schemes in the literature deal with the synchronisation problem.

In [12], an adaptive synchronisation method consisting of computing an index to maximise a function which depends on the alignment of the embedded mark and the test signal is presented. This method is shown to be robust against different attacks, but requires the computation of the alignment index for each sample, which increases the computational time and makes its application in real-time systems difficult. A different technique for synchronisation is suggested in [13], which performs an embedding procedure which works with the whole original signal and requires a cycle correlation operation to be performed at the detector. This mechanism implies the calculation of cyclic convolution via an FFT algorithm. Liu and Inoue [14] uses the spread spectrum technology in which the mark is represented by patterns consisting of sinusoids which are phase-modulated by the elements of a pseudo-random sequence. In this method, special header patterns are used to recover the synchronisation by maximising the autocorrelation. In order to compute this autocorrelation, [14] suggests using the FFT with the re-sampling technique and, though this approach can be quite efficient, it will probably involve more computational burden than most time-domain synchronisation approaches. Ref. [15] suggests a watermarking scheme with inherent robustness against desynchronisation, since the mark is embedded in the average of the low-frequency sub-band coefficients of the discrete wavelet transform (DWT). However, no specific method to recover the synchronisation of the embedded bits is presented. In [16], a method which embeds both the

synchronisation and the informational marks in the discrete cosine transform (DCT) domain is presented. In order to detect the synchronisation segments, the DCT must be applied within the search iteration, making it unsuitable for real-time applications. In [17], a method which embeds the information mark in the largest energy region of the DWT transform is presented. This method is based on the assumption that the acceptable attacks, especially those consisting of cropping parts of the signal, leave those DWT coefficients unchanged. On the other hand, the synchronisation is achieved applying some statistical methods to estimate the possible scale changes and/or delays applied to a hypothetically attacked signal. Hence, no specific synchronisation marks are applied, but some correlation indexes between the marked and the test signal are maximised. The method presented in [18] embeds both the synchronisation and the information marks in the coefficients of the low-frequency sub-band of the DWT transform, resulting in an enhanced robustness against common signal processing attacks. In addition, this method exploits the time-frequency localisation feature of the DWT transform to reduce the computational burden required for the search of the synchronisation marks. However, this method requires the modification of the segmentation of the test signal in case that the synchronisation mark is not retrieved in each segment, which may be excessively time consuming for mark retrieval in real-time applications.

Audio watermarking schemes with a time-domain synchronisation code and a separate watermarking segment have been suggested in the literature [19, 20]. In [19], the synchronisation code is the 12-bit Barker code "111110011010" which is embedded in the 13 least significative bits (LSB) of 12 consecutive audio samples. Although this allows synchronisation to be performed in a very efficient way, the perceptual quality is damaged with many audible clicks at the synchronisation positions. This method was improved in [20], where the 16-bit Barker code "1111100110101110" is embedded by modifying the average of a few consecutive samples (five samples in the experiments given in [1]). In fact, the average of these samples is quantised such that an odd number means a "1" and an even number is a "0". Hence, the quantisation step determines the perceptibility of the mark. However, some audio files require a large quantisation step to ensure robustness, which results, again, in audible clicks at the synchronisation positions. The advantage of this kind of synchronisation marks [19, 20] is that the search can be performed in the time domain, without computing any kind of transform. As the information mark is concerned, [20] embeds the information mark in the DWT and DCT transform domains. The watermark extraction methods consists of exploring the test signal to locate a synchronisation mark. Once such a mark has been found, the DWT and DCT transforms are used to extract the information mark. The audible clicks introduced by both methods can be explained by the easily noticeable peak distortions they introduce in some samples.

From a computational point of view, the ideas of [19, 20] provide a more efficient synchronisation compared to the other referred schemes, but the significant audible distortions introduced by them are a relevant drawback when transparency is an intended property. In [1], we propose a novel time domain

Scheme	Content	Sync	SNR (dB)	Payload (bps)
[19]	Short clips	Yes	43.0	36
[20]	Short clips	Yes	43.1	–
[9]	SQAM clips	No	42.8	2
[10]	Song	No	$30 - 45$	86
[11]	Song	No	25	43
[1]	**Song + Quartet + SQAM clips**	**Yes**	**25.70**	**30.73**

Table 1.1: Comparison of the chosen schemes with the proposed [1] in terms of SNR and capacity

synchronisation technique. The chosen approach makes it possible to use the detector algorithm in real-time applications, due to the efficiency of the time domain search of the synchronisation marks. In addition, it provides excellent imperceptibility and robustness results, as shown in the experiments. Apart from the self-synchronisation strategy, we present a novel watermarking scheme for the information mark. The new scheme stems from the results of the schemes presented in [21, 22, 23], since it works in the fast Fourier transform (FFT) domain by introducing (small) modifications in the amplitude at some selected frequencies. In addition, the detector for the new scheme is blind (in contrast to those of [21, 22]) and its execution is fast enough to be used in real-time applications. Furthermore, the modifications introduced in the FFT domain during the embedding process are minimal and the sorting of the FFT amplitudes is preserved, resulting on an excellent imperceptibility whilst keeping robustness for the most usual signal processing attacks, as shown in the experiments.

The suggested scheme [1] is compared with other self-synchronised [19, 20] and not self-synchronised [10, 9, 11] methods. Table 1.1 shows the capacity and SNR results of the suggested scheme and the selected methods. [20] reports that a 64×64 (black and white) image is embedded in the audio clips, but they do not report a specific number of hidden bits per second. All the other schemes (including the suggested one) yield very similar capacity results.

Unfortunately, the selected schemes do not report transparency results in terms of ODG and they just compute SNR values. In order to overcome this drawback, we have implemented the schemes of Table 1.1 which provide time-domain synchronisation [19, 20] to provide a fair comparison and to analyse the ODG of these schemes. The implementation has been performed in such a way that the all three schemes have *exactly the same capacity* (30.73 bps) to provide a fair comparison.

The result of this comparison in terms of transparency is given in Table 1.2. The columns "Clicks" report whether audible clicks can be heard or not in the marked files and "Tr." shows if the marked file can be considered transparently marked or not ("Yes" means ODG $\gtrapprox -1$ and no annoying clicks). The minimum

Title	Genre	[1]			[19]			[20]		
		ODG	**Cl.**	**Tr.**	**ODG**	**Cl.**	**Tr.**	**ODG**	**Cl.**	**Tr.**
Floodp.	E. folk	**0.00**	**No**	**Yes**	−0.31	Yes	No	−0.05	Yes	No
Stop P.	E. folk	**0.00**	**No**	**Yes**	−0.61	Yes	No	−0.11	Yes	No
Rust	E. folk	**−0.10**	**No**	**Yes**	−0.67	Yes	No	−0.15	Yes	No
Canon	Quartet	−0.17	**No**	**Yes**	−0.31	Yes	No	**0.00**	Yes	No
Bass	Voice	−1.07	**No**	**Yes**	−0.05	Yes	No	**0.00**	Yes	No
Violin	Instr.	−0.55	**No**	**Yes**	**−0.08**	Yes	No	−0.12	Yes	No

Table 1.2: Transparency comparison with our method [1] for the same capacity (30.73 bps)

ODG for each file is highlighted in boldface. Among the self-synchronising schemes analysed in this table ([19, 20] and the proposed scheme [1]), only the proposed method does not produce annoying audible clicks at the position of the synchronisation marks. The comparative results for six files of the family of time domain audio signals are given in Table 1.2. It can be noticed that, despite the favourable conditions for the other two schemes, our proposed scheme [1] still produces the best ODG for the electric folk (pop) music files. The results for the quartet classical music is still acceptable, though [20] provides better results, and the pure instrument and voice files would require a more specific tuning. The ODG for these two files can be easily improved with an appropriate tuning. In addition, it is worth remarking that both [19, 20] produce annoying audio clicks at the synchronisation points, whereas the synchronisation scheme of the proposed scheme is completely transparent.

Table 1.3 compares the robustness of the chosen and the proposed schemes, where the "ODG" column shows the average ODG obtained for these nine attacks for the six test files. All of these schemes provide similar robustness for the chosen set of attacks. Note that the robustness results are given in bit error rate (BER) form which is common for the reported works. For the proposed scheme, the BER is not directly obtained since repeat coding and error correcting codes are used as detailed above. The BER values displayed in the table for the suggested scheme are 0 when the mark is recovered (since it is only considered recovered if all bits are correct) and 50% (which is the worst possible value) when the attack is considered successful (only for the re-sampling 11.025 kHz attack), although the real BER value would not be so large. This table shows that the robustness of our suggested scheme [1] is comparable to that of recent audio watermarking systems.

Attack	**ODG**	**Robustness** (BER %)					
		[1]	[19]	[20]	[9]	[10]	[11]
Re-quantisat.	−2.14	**0**	0	0	0	–	0.5
Re-samp. 22.05 kHz	−1.10	**0**	49	0	0	0	1
Re-samp. 11.025 kHz	−3.29	$\sim$ **50**	49	1	–	0	–
Additive noise	−3.24	**0**	3	1	0	0	2
10% cropping	NA	**0**	0	0	0	–	–
Low-pass filters	−0.15 (RC) −1.60 (But.)	**0** (10 kHz)	–	–	10-15 (6-8 kHz)	1 (20 kHz)	1, 2 (12, 8 kHz)
MP3 128 kbps	−0.64	**0**	0	0	0	0	1
MP3 112 kbps	−0.93	**0**	0	0	0	0	–
MP3 96 kbps	−1.38	**0**	–	0	0	0	2

Table 1.3: Comparison of the chosen schemes with our method [1] in terms of robustness

1.2 High capacity audio watermarking using the high frequency band in the discrete wavelet domain

Many audio watermarking schemes take advantage of the properties of the human auditory system (HAS) and different transforms, resulting in various techniques such as embedding algorithms based on low-bit coding, echo, patchwork [11], rational dither modulation [24], Fourier transform [23, 4], quantization [25, 26, 27] and the wavelet transform [28, 20].

Considering the embedding domain, audio watermarking techniques can be classified into time domain and frequency domain methods. Time domain watermarking schemes are relatively easy to implement and require less computing resources compared to transform domain watermarking methods. On the other hand, time domain watermarking systems are usually weaker against signal-processing attacks compared to the transform domain counter- parts. Phase modulation [29] and echo hiding [30] are well known methods in the time domain.

In frequency domain watermarking, after taking one of the usual transforms such as the Discrete/Fast Fourier Transform (DFT/FFT) [23, 4], the Modified Discrete Cosine Transform (MDCT) or the Wavelet Transform (WT) [28, 20, 18, 9] from the signal, the hidden bits are embedded into the resulting transform coefficients. For example, [9] takes advantage of the mean of absolute values to design a scheme which has capacity equal to 40 bits (which are embedded in a 20-second audio signal in the experiments given in [3]), and robustness against common attacks. In [23, 4] the FFT domain is selected to embed watermarks for making use of the translation-invariant property of the FFT coefficients to resist

small distortions in the time domain. In particular, [23, 4, 28, 20, 18, 9] show that the frequency domain provides excellent robustness against attacks. In fact, using methods based on transforms provides a better perception quality and robustness against common attacks at the price of increasing the computational complexity.

In our proposed schemes [2] and [3], the last high frequency band of the second level wavelet decomposition (DD), for which the HAS is not very sensitive to alteration, is used for embedding. The experimental results show that high capacity, remarkable transparency and robustness against most of common attacks are achieved.

Figure 1.1 illustrates the effect of various attacks provided in the Stirmark Benchmark for Audio v1.0 [31] on ODG and the BER for five audio signals. The synchronization [20] which is robust against common attacks and the embedding method described have been used and, then the SMBA software has been applied to attack the whole marked files. Finally, the attacked file is scanned in time domain to find the synchronization codes then the secret information of each clip is extracted. The ODG in Figure 1.1 is calculated between the marked and the attacked-marked files. The parameters of the attacks are defined based on SMBA web site [31] for the scheme proposed in [3]. Other schemes may use different parameters. For example, in AddBrumm, 1-5 k shows the strength and 1-6 k shows the frequency. This row illustrates that any value in the range 1-5 k for the strength and 1-6 k for the frequency could be used with slight changes in BER. In fact, this table shows the ranges (the worst and best) of ODG and BER for the five test signals. When the BER is (slightly) greater than zero, it can be made zero by using Error Correction Codes at the price of reducing the capacity. The BER column for proposed scheme shows the total BER after embedding synchronization mark and watermark. E.g. the BER of the BassBoost attack changes from 0 to 2 without considering the synchronization however BER is increased to 6 to 14 after using synchronization.

Only a few attacks such as Pitchscale and TimeStretch in Figure 1.1 remove the hidden data (BER $< 15\%$). Note, however, that the ODG of these attacks are extremely low (about -3.5). This means that these attacks do not only remove the hidden data, but also destroy the perceptual quality of the host signal.

In Table 1.4, we compare the performance of recent audio watermarking strategies, which are robust against common attacks, with our methods in [3] and [2]. [24] measures distortion using the mean opinion score (MOS), which is a subjective measurement, and achieves transparency between imperceptible and perceptible but not annoying (MOS=4.7). [25, 18] propose low capacity schemes, but they are robust against most common attacks. In particular, [18] is robust against most common signal processing and attacks, such as Gaussian noise, re-sampling, re-quantization, and MP3 compression. Although the chosen schemes from the literature use different audio signals and attack parameters, the properties of each algorithm in capacity of embedding secret information and transparency are summarized in Table 1.4, and robustness against attacks is shown in Figure 1.1. The comparison shows that the compared schemes are

Attack name	ODG of attacked file	Parameters	BER %						
			Proposed	A	B	C	D	E	F
AddBrumm	−3.1 to−3.7	1–5 k, 1–6 k	0 to 1	–	0	0 to 1	–	–	–
AddDynNoise	−2.1 to−2.5	1–2	2 to 7	–	2	0 to 8	–	–	–
ADDFFTNoise	−0.3 to−0.1	2048,400	0 to 2	–	1	1 to 2	–	–	–
Addnoise	−0.8 to−0.4	1–20	0 to 6	2	1	0 to 1	–	0	5 to 25
AddSinus	−3.1 to−2.5	1–5 k,1–7 k	0	–	0	0	–	–	–
Amplify	−0.2 to−0.0	20–200	0 to 1	–	0	0	–	–	–
BassBoost	−3.8 to−3.3	1–50,1–50	6 to 14	–	–	0	–	–	–
Echo	−3 to−1.3	1–5	1 to 28	1.2	63	0 to 1	–	6	–
FFT_HLPassQuick	−3.7 to−3.3	2048,1–10 k,18 k–22 k	12 to 17	–	5	1 to 4	–	–	–
FFT_Invert	−3.8 to−3.1	1024	0	–	2	1 to 2	–	–	–
FFT_RealReverse	−3.5 to−3	2-2048	14 to 29	–	–	–	–	–	–
FFT_Stat1	−3.6 to−2.9	2-2048	21 to 37	–	1	–	–	–	–
Invert	−3.6 to−2.8	–	0	–	–	0	–	–	–
Resampling	−2.1 to−1.8	44/22/44	7 to 11	1	0	5	0	0	0
LSBZero	−0.2 to 0.0	–	0	–	0	0	–	0	–
MP3	−0.4 to 0.0	≥128	0 to 2	0.3	–	0 to 5	0	–	1
Noise_Max	−0.4 to−0.1	1–2,1–14 k,1–500	1 to 4	–	–	0 to 1	–	–	–
Pitchscale	−3.7 to−3.1	1.1	31 to 51	–	–	0 to 1	–	–	–
RC_HighPass	−3.7 to−3.1	1–14 k	0 to 5	–	–	0 to 1	–	–	–
RC_LowPass	−3.8 to−0.4	2 k–22 k	0 to 8	2	0	0	0	3	–
Smoth	−3.6 to−3.3	–	14 to 22	–	–	–	–	–	–
Stat1	−2.1 to−1.4	–	9 to 12	–	8	–	–	–	–
TimeStretch	−3.8 to−3.2	1.05	34 to 61	–	–	–	–	–	–
Quantization	−0.6 to−0.2	16–12	5 to 9	0.5	–	–	0	0	0

Figure 1.1: Robustness test results for five selected files and comparison with schemes in this literature: Proposed [3], A [11], B [24], C [23], D [28], E [25], F [18]

robust against common attacks and transparency is in an acceptable range, about 30 dB. However, the capacity of these schemes is just a few hundred bps (except for the method suggested in [23]). This comparison shows that the capacity of the proposed schemes [3] and [2] is very remarkable, whilst keeping the transparency and BER in their acceptable ranges.

Table 1.4: Comparison of different watermarking algorithms with our methods in [2] and [3]

Algorithm	Audio file	SNR (dB)	ODG of marked	Payload (bps)
[11]	Song	25	–	86
[24]	Song	–	–	689
[23]	Song	30.5	−0.6	2996
[28]	Song	30	–	172
[25]	Classical music	25	–	176
[18]	Song	25-40	–	172
[2]	Song	33	−0.5	5501
[3]	Song	30	−0.7	11002

1.3 High capacity FFT-based audio watermarking

Considering the embedding domain, audio watermarking techniques can be classified into time domain and frequency domain methods. In frequency domain watermarking [9, 32, 24, 23, 4, 5, 2], after taking one of the usual transforms such as the Discrete/Fast Fourier Transform (DFT/FFT) [4, 5, 2], the Modified Discrete Cosine Transform (MDCT) or the Wavelet Transform (WT) from the signal [2, 33, 20], the hidden bits are embedded into the resulting transform coefficients. In our papers [4, 5, 2] the FFT domain is selected to embed watermarks for making use of the translation-invariant property of the FFT coefficients to resist small distortions in the time domain. In fact, using methods based on transforms provides better perceptual quality and robustness against common attacks at the price of increasing the computational complexity.

The experimental results show that our methods [5] and [6] provide robustness against common signal processing attacks and entail very low perceptual distortion.

Our methods [5] and [6] have been compared with several recent audio watermarking strategies. Almost all the audio data hiding schemes which produce very high capacity are fragile against signal processing attacks. Because of this, it is not possible to establish a comparison of the proposed scheme with other audio watermarking schemes which are similar to it as capacity is concerned. Hence, we have chosen a few recent and relevant audio watermarking schemes in the literature.

In Table 1.5, we compare the performance of the proposed watermarking algorithms and several recent audio watermarking strategies robust against the MP3 attack. [9, 32, 33] have low capacity but are robust against common attacks. [24] Evaluates distortion by mean opinion score (MOS), which is a subjective measurement, and achieves transparency between imperceptible and perceptible but not annoying (MOS = 4.7). Capacity, robustness and transparency are the three main properties of an audio watermarking scheme. Considering a trade-off between these properties is necessary. E.g. [9] proposed a very robust, low capacity and high distortion scheme. However [24] and the proposed schemes lead to high capacity and low distortion but they are not as robust as the low-capacity method described in [9]. Our scheme [23] has good properties, but the scheme proposed in [6] can manage the needed properties better since there are three useful adjustable parameters. For example, in [6] by using frame size of $d = 8$ getting robustness against MP3-64 is easy. On the other hand, in [23], low bit rate MP3 compression was not considered.

Table 1.5: Comparison of different watermarking algorithms with our methods [5] and [6]

Algorithm	Capacity (bps)	Impercep. in SNR (dB)	Impercep. (ODG)
[9]	2	42.8 to 44.4	-1.66 to -1.88
[33]	2.3	Not reported	Not reported
[32]	4.3	29.5	Not reported
[23]	2996	30.55	-0.6
[24]	689	Not reported	Not reported
[5]	1478 to 8719	35.2 to 44.6	-0.18 to -0.78
[6]	506 to 4025	29 to 46	-0.1 to -1.5

This comparison shows the superiority in both capacity and imperceptibility of the suggested methods with respect to other schemes in the literature. This is particularly relevant, since the proposed schemes are able of embedding much more information and, at the same time, introduce less distortion in the marked file.

1.4 High capacity logarithmic audio watermarking

The watermarking scheme should not affect the perceptual quality of audio. In [7], this is achieved by using a psychoacoustic model in order to guarantee that the watermarking process does not distort the cover audio signal.

Several research results exist for watermarking in the logarithm and cepstrum domains. Lee et al. [34] introduced a digital audio watermarking such that the watermark is embedded into cepstrum coefficients of the audio signal based on spread spectrum. Li and Yu [35] suggested a robust and transparent

audio data embedding method in cepstrum domain. BCH code-based robust audio data hiding in the cepstrum domain is presented in [36]. Hsieh et al. [37] suggested the audio watermarking technique based on time energy features. Li et al. [38] proposed an audio watermarking scheme in the cepstrum domain based on statistical mean manipulation. Hu and Chen [39] proposed cepstral watermarking that manipulates the statistic mean. [40] suggested a digital watermarking method based on log-scaling of frequency in the decoding process for robust detection. [41] is the first technique on applying log-polar mapping to audio watermark. The log-polar mapping is only applied to the frequency index, not to the transform coefficients.

Watermarking methods based on the human auditory system (HAS) have been suggested in some previous works such as [42, 43, 44]. In our papers [23, 5], the Discrete/Fast Fourier Transform (DFT/FFT) domain is selected to embed watermarks for taking benefit of the translation-invariant property of the FFT coefficients to resist small distortions in the time domain. In [7] we propose an audio watermarking algorithm in the logarithm domain based on the HAS. To evaluate the performance of the proposed method and to consider the applicability of the scheme in a real scenario, the album Rust by No, Really [45] has been used.

In Table 1.6, we compare the performance of our proposed watermarking algorithm [7] and several recent audio watermarking strategies robust against the MP3 attack.

Table 1.6: Comparison of different watermarking algorithms with our proposed method [7]

Algorithm	Capacity (bps)	Impercept. in SNR (dB)	Impercept. (ODG)
[46]	8	Not reported	$-3 < \text{ODG} < -1$
[47]	64	30-45	$-1 < \text{ODG}$
[23]	3k	30.55	-0.6
[5]	1.5-8.5k	35-45	$-0.8 < \text{ODG} < -0.1$
[7]	800 to 7k	21 to 36	$-1 < \text{ODG} < -0.1$

Speech applications and codecs are considered in [46]. The distortion introduced to the marked signal is slightly annoying, capacity is very low and robustness is achieved against compression attacks. Recently, [47] introduces a very fast scheme which uses the Fourier transform. The embedding bit-rate is low, 64 bits per second, but the scheme is very robust against several attacks. Our methods [23, 5] have a remarkable performance in the different properties, but the scheme proposed in [7] can manage the needed properties better, since there are three useful adjustable parameters. In particular, the results of [7] make it possible to improve the transparency results with respect to [23, 5] due to the explicit use of the HAS and adaptive quantization. This comparison shows the superiority in both capacity and imperceptibility of the suggested method [7] for the same robustness with respect to other robust schemes. This is particularly relevant, since the proposed scheme can embed much more infor-

mation and introduces less distortion in the marked file.

Chapter 2

Watermarking of speech

This chapter presents the evaluation of the related work in the speech watermarking field. This chapter consists of a single section which summarizes the work performed in the following article:

[48] M. Fallahpour, D. Megías, and H. Najaf-Zadeh, "Adaptive speech watermarking in wavelet domain based on logarithm," in *SECRYPT*, pp. 412–415, 2012.

2.1 Adaptive speech watermarking in the wavelet domain based on logarithm

Speech watermarking systems usually embed watermarks in inaudible parts of the speech signals. Many speech watermarking and information embedding schemes have been proposed. These methods can be classified into seven approaches: least significant bit, phase coding, echo hiding analysis by synthesis-based, spectrum techniques in the transform domain, feature-based and watermarking combined with coding frames.

Several quantization-based methods have been proposed in the recent years by using discrete Hartley transform coefficients [49], autoregressive model parameters [50], and the pitch period [51]. The payload range of those systems is from a few bits to a few hundred bits per second, with varying robustness against different types of attacks.

The method proposed in [48] takes advantage of the wavelet transform, which divides the signal into low and high frequency bands. The signal-to-noise ratio (SNR) values in the low frequency region are in the range of 15 to 20 dB, and gradually decreases to zero as the frequency increases. To achieve robustness, using the low frequency bands is more advisable, whereas embedding the watermark in high frequency bands leads to better transparency.

The experimental results show that the distortion caused by the embedding algorithm is adjustable and lower than that caused by the ITU-T G.723.1 speech

codec [52]. G.723 is a standard speech codec that guarantees the quality of compressed speech and thus, it is evident that the marked signal has high quality (PESQ-MOS around 4, i.e., near transparent). The embedding rate is adjustable and ranges from very low bit-rates to 4000 bits per second (bps).

Four male speech files sp01.wav - sp04.wav and five female files sp11.wav - sp15.wav taken from the Noizeus speech corpus [53] have been selected for our experiments. The sampling frequency is 8000 Hz and each sample is represented with 32 bits.

In Table 2.1, we compare the performance of the proposed watermarking algorithm [48] and several recent speech watermarking strategies. In [49], the MOS of the narrow band (NB) speech is 3.7 and the MOS of the NB speech with embedded data is 3.625. The small difference between the MOS results demonstrates the transparency of the proposed data-embedding scheme. In simulations, the embedding data rate is 600 information bits/second. The method of [51] allows a relatively low embedding capacity (about 3 bps), which is suitable for metadata tagging and authentication applications. However, [51] is robust with low data-rate (5-8 kbps) speech coders. The focus of [54] is on the robustness performance of linear prediction embedded speech watermarking. The technique in [48] is robust to a wide range of attacks including noise addition, cropping, compression, and filtering, but the achieved capacity is low.

Table 2.1: Nonlinear Model Results

Algorithm	SNR(dB)	PESQ-MOS	Payload (bps)
Sagi and Malah [49]	35	3.6	600
Celik et al. [51]	–	–	3
Girin and Marchand [55]	High	–	200
Gurijala and Deller [54]	–	–	24
Proposed [48]	**30-40**	**$\sim$ 4**	**800-4000**

Chapter 3

Reversible watermarking of images

This chapter presents the evaluation of the related work in the reversible image watermarking field. The structure of the chapter is as follows:

- Section 3.1 is based on the following paper:

  [56] M. Fallahpour and D. Megías, "Digital watermarking," ch. Reversible Data Hiding Based On H.264/AVC Intra Prediction, pp. 52–60, Berlin, Heidelberg: Springer-Verlag, 2009.

- Section 3.2 is based on the following paper:

  [57] M. Fallahpour, D. Megías, and M. Ghanbari, "Subjectively adapted high capacity lossless image data hiding based on prediction errors," *Multimedia Tools Appl.*, vol. 52, no. 2-3, pp. 513–527, 2011.

  [58] M. Fallahpour, D. Megías, and Y. Q. Shi, "Lossless image data embedding in plain areas," pp. 78800H–78800H–8, 2011.

- Finally, Section 3.3 is based on the following papers:

  [59] M. Fallahpour, D. Megías, and M. Ghanbari, "High capacity, reversible data hiding in medical images," in *Proceedings of the 16th IEEE international conference on Image processing*, ICIP'09, (Piscataway, NJ, USA), pp. 4185–4188, IEEE Press, 2009.

  [60] M. Fallahpour, D. Megías, and M. Ghanbari, "Reversible and high-capacity data hiding in medical images," *Image Processing, IET*, vol. 5, pp. 190 –197, march 2011.

3.1 Reversible Data Hiding Based On H.264/AVC Intra Prediction

New findings of data hiding in digital imaging open wide prospects of new techniques in modern imaging science, secure communication and content management. Data hiding has been proposed as a promising technique used for security, authentication, fingerprint, video indexing, error resilient coding, etc.

H.264/AVC [61] is the newest international video coding standard providing many techniques to improve the coding efficiency of intra and inter frames. Among many new techniques, the intra prediction technique is considered as one of the most important features in the success of H.264/AVC. This technique, which is used in the proposed method, increases the dependence of the neighbouring blocks. An error resilient method that embeds information into image or video itself is another technique used in H.264/AVC. Once an error is detected, the error resilient technique extracts the hidden information and recovers the error block. Using reversible information embedding in the error resilient causes the original digital content to be completely restored in the decoder and also results in a lossless extraction of the embedded data.

Reversible data hiding [62] is a novel category of data hiding schemes. The reversibility is essential to some sensitive applications such as medical diagnosis, remote sensing and law enforcement. The methods reported in [63, 64, 65, 66, 67, 68, 69] are considered among the best schemes in lossless data hiding. In [70], a high capacity lossless data hiding method was proposed based on the relocation of zeros and peaks of the histogram of the image blocks to embed the data. Recently, Lin and Hsueh [63] presented a reversible data hiding method based on increasing the differences between two adjacent pixels to obtain a stego-image with high payload capacity and low image distortion. Among recent lossless methods performed on the transform domain, the schemes based on the integer wavelet transform domain are more notable. Tian [64] used the integer Haar wavelet transform and embedded the secret message into high-frequency coefficients by difference expansion. Kamstra and Heijmans [65] improved Tian's method by using the information in the low-frequency coefficients to find suitable expandable differences in the high-frequency coefficients. Xuan et al. [67] reported the lossless embedding algorithm carried out in the integer wavelet transform domain. Xuan et al. [66] proposed a lossless data hiding scheme based on optimum histogram pairs in the wavelet domain. Recently, a few prediction based data hiding methods have been proposed [68, 69]. Thodi et al. [68] expanded the difference between a pixel and its predicted value in the context of the pixel for embedding data. In Kuribayashi et al.'s algorithm [69], a watermark signal is inserted in the LSB of the difference values between pixels.

The method proposed in [56], called SIPE, is based on increasing the differences between pixels of the cover image and their intra prediction values. The SIPE method consists of an embedding and a extracting procedure. The embedding process includes both computing the prediction errors and embedding the information bits in the shifted prediction errors. Moreover, the data extraction

is the reverse of data embedding.

The SIPE algorithm was implemented and tested on various standard test images from the UWaterloo database [71]. Also, the results of Lin and Hsueh's [63], Kamstra and Heijmans's [65], and Xuan et al's. [66] methods were compared with the results obtained with this method. This comparison shows that the SIPE method is able of hiding more secret data than almost all methods mentioned in the literature for the same (above 45dB) PSNR. The experimental results of the SIPE method show that the embedded data remains invisible, since no visual distortion can be revealed. It is worth pointing out that the embedded data were generated by the random number generator in MATLAB on a personal computer.

Figure 3.1 illustrates the performance comparison of the SIPE with the methods reported in [63], [65], and [66] for the Lena image in terms of PSNR (dB) and payload (bpp: bits per pixel). As shown in Fig 3.1, the SIPE scheme provides high enough bound of the PSNR (above 48dB) with a quite large data embedding capacity, indicating a fairly better performance of the SIPE method.

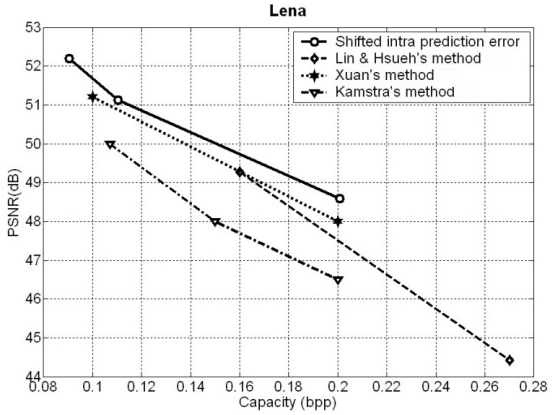


Figure 3.1: Comparison of the embedding capacity (bpp) and distortion (PSNR) for the Lena image among Lin & Hsueh's method [63], Xuan's method [66], Kamstra's method [65] and our proposal SIPE [56]

3.2 Lossless image data hiding

Data hiding methods can conceal additional information in media. Most data hiding schemes distort the cover media in order to embed the secret data. Although the distortion is often small and imperceptible, the reversibility is crucial to some sensitive applications. In applications, such as in law enforcement, medical image systems, it is required to be able to reverse the marked image back to the original cover image for legal consideration. In remote sensing and military imaging, high accuracy is demanded. In some scientific research, experimental

data are expensive to be achieved. Under these circumstances, the reversibility of the original media is desired. Reversible data hiding [72, 62] is a novel category of data hiding schemes, where at present, there are growing interest in their lossless version.

For the purpose of increasing the embedding capacity, Fridrich et al. [73] presented a new lossless data hiding method based on modifying the least significant bits (LSBs). Their algorithm compresses the least significant bit plane of the cover image and then mixes them alongside the embedded data into the cover image. To improve the data hiding potential of Fridrich et al.'s method, Celik et al. [74] proposed a generalized-LSBs algorithm where the quantization residues of the cover image after the CALIC (context-based adaptive lossless image codec) lossless compression algorithm is used to generate the compressed residues. The remainder of the compression space is used to embed the secret information.

A main category of high-capacity reversible data-embedding algorithms may be classified as expansion-embedding approaches. A common aspect of these approaches is the use of some decorrelating operators to make features with small magnitudes. The data embedding process is done by expanding these features in order to prepare vacancies into which the data bits are embedded. The first algorithm in this category was proposed by Tian [64] and then improved by [75, 65], and [76]. Tian [64] suggested a difference-expansion (DE) scheme that divides the image into pairs of pixels within three groupsexpandable, changeable, and nonembeddablein which information was recorded using a location map. In this method, one hidden bit can be embedded into one of the changeable or expandable pairs. A generalized version of Tian's scheme was enhanced by Alattar [75] to improve the payload, in which instead of pixel pairs the difference expansion of vectors is used. Kamstra et al. [65] have also extended Tian's method by using the information in the lowpass band to find appropriate expandable differences in the high-pass band.

Kim et al. [76] improved [65, 64] by introducing a new location map and a new embedding method. Chang et al. [77] suggested a reversible embedding scheme for side match vector quantization (SMVQ) compressed images. Their scheme can recover only the SMVQ image instead of the vector quantized (VQ) image. Chang and Lin [78] introduced a completely reversible embedding scheme for VQ compressed images. However, the computational cost of their method is high, and it is not suitable for real-time applications.

Following the methods of LSB, difference-expansion and vector quantization algorithm groups, the last category of data hiding reported in[70, 63, 79, 66] and [67] which have attracted great interests in recent years began by the work of Ni et al. [79]. The main idea in this category is to use distribution of numbers. These numbers can be the original values of pixels, transformed pixels, etc. Ni et al. [79] introduced a lossless data embedding algorithm based on the spatial domain histogram shifting. An extension to Ni et al work was carried out in [70], where a higher capacity was achieved by relocation of zeros and peaks of the image histogram in image blocks. Lin and Hsueh [63] presented a reversible method based on increasing the differences between two adjacent pixels. Xuan

et al. [67, 66] reported a remarkable reversible method where operations are carried out in the integer wavelet transform domain.

Gao et al. [80] use average of differences between pixels of non-overlap image blocks and the block skipping scheme as well as a novel parameter model to guarantee the lossless recovery of the original image. They claim that the method is robust against salt-and-pepper noise and has the potential for capacity adjustment. Algorithm in [81] utilizes a peak point of image histogram and the location map which increases amount of embedding information of [79] at the price of distortion. In [82] a simple and efficient reversible data hiding algorithm is presented which uses the histogram of the differences between sub images obtained through subsampling to enhance [79]. Recently Hong et al. [83] take advantages of median edge detector to design a scheme based on histogram shifting. Tsai et al. [84] with a predictive coding algorithm propose a technique for medical images which improves Ni et al. [79] for some images by about 1.5 dB. However performance of their method is image content dependent and for some images under the same capacity, the quality is poorer than [79].

In these algorithms although through use of prediction, the capacity is improved, but less consideration is paid on the acceptable quality of marked images. What would be more useful, if the capacity could be increased up to the level that marked image quality is still acceptable. This is what we intend to do in [57], where the embedding capacity is traded for marked image quality.

Our proposed method [57], named adaptive shifted prediction error (ASPE), is based on hiding data at the locations of larger differences between the pixels of the cover image and their prediction values, to gain from spatial masking of the human visual system.

From the literature on prediction techniques, the median edge detector (MED) [85] and the gradient adjusted prediction (GAP) [86] are the states of the art pixel predictors that are used in LOCO-I (Low Complexity Lossless Compression for Images) and CALIC image encoders, respectively. In 2000, Jiang et al. [87] proposed a predictor that can be thought of as a modified version of MED.

Considering the GAP is the best predictor of all, we now compare the performance of the ASPE with the GAP predictor against the well known high capacity data hiding schemes reported in the literature, such as [70, 65, 63, 79, 64, 66], and [76]. Figure 3.2 contrasts the performance of ASPE (with the GAP prediction) against these methods for Lena and Barbara images in terms of PSNR and data hiding payload (bpp: bits per pixel). The figure clearly shows the superiority of the ASPE over the other methods. The embedding capacity was limited for a minimum 40 dB in quality.

One of the main features of our scheme is that the quality of marked image is impaired proportional to the required capacity. However, ASPE has also additional advantage that the rate of decay of impairment is small. To verify this, we implemented this trade off on the Ni et al. [79], Hong et al. [83], and Tsai et al. [84] schemes such that frequencies were chosen for the required capacity for Lena and Barbara images, shown in Fig. 3.3. As the figure shows, while for a capacity of 5 kbits, with Ni et al. [79] PSNR=47.8 dB, and that of ASPE is

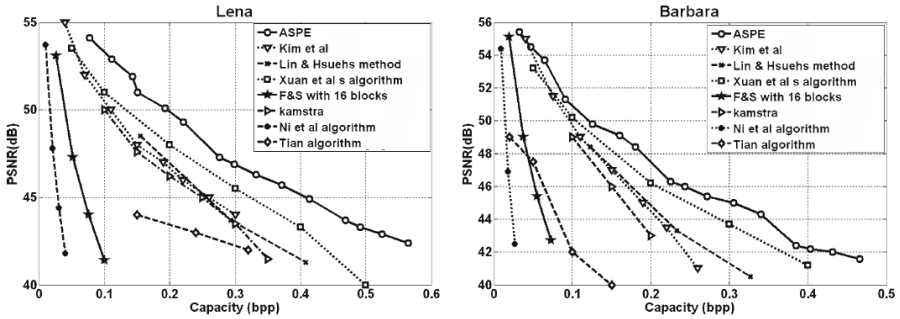


Figure 3.2: Comparison for Lena and Barbara images the following reversible methods: Kim et al. [76], Lin & Hsueh [63], Xuan et al [66], F & S [70], Kamstra [65], Ni et al [79], Tian [64], and our proposal ASPE [57]

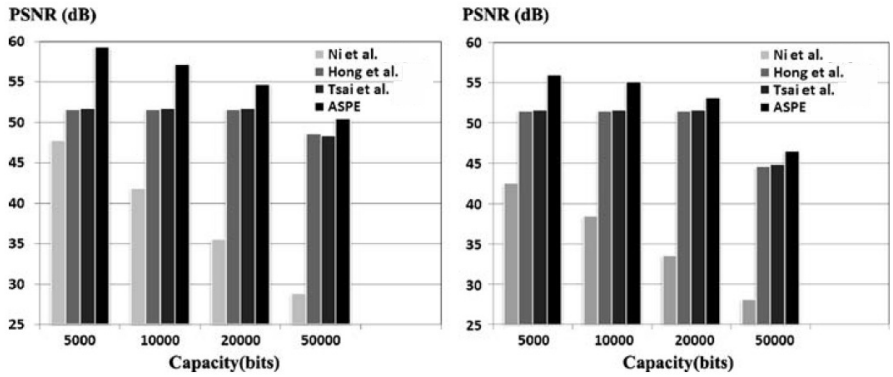
59.4 dB, when the capacity is increased to 50 kbits, the quality of the marked image under [79] is dropped below 27 dB, but that of ASPE at this rate is more than 46 dB. However, the PSNR in Hong et al. [83] and Tsai et al. [84] schemes are much better than [79], as shown in Fig. 3.3, but they are still inferior to ASPE. The main problem with these methods is the lack of efficiency, as both methods suffer the same distortion at 5 and 20 Kbits, which means the data embedding method is not capacity efficient.

This is not the case with ASPE and [79], where increasing the capacity the marked image quality degrades accordingly. Moreover the subjective quality of the marked image under ASPE is very good, even at very low PSNRs.

We have also proposed a method for lossless image data embedding in plain areas [58] that makes use of the histogram for data hiding.

Use of histogram of image for data hiding was first introduced by Ni et. al [79]. Shift all pixels which they are larger than peak of the histogram to prepare a space for embedding secret information is the main idea of [79]. The peak point of the histogram defines the capacity of the scheme. Then in [70, 63, 88] through image tiling, difference between pixels and prediction the data hiding capacity was increased by narrowing the histogram. The key point in the histogram based algorithms is that the narrower histogram results in the more capacity for data hiding. This is because a narrower histogram has a higher peak. Hence it is expected the histogram of the prediction error of an image to be able to accommodate more data than the histogram of the image itself. In all these schemes [79, 70, 63, 88] to prevent error in extracting the embedded data and reversibility, all values larger than peak point have to be incremented which increases the distortion. The aim of the scheme we propose in [58] is decrease the amount of modified pixels to improve transparency by keep their values in the edges of the image which leads us to a better capacity and better transparency.

Fig. 3.4 illustrates the performance comparison of the scheme in [58], with



(a) Lena (b) Barbara

Figure 3.3: Rate of trade off in capacity versus quality between Ni et al. [79], Hong et al. [83], Tsai et al. [84] and our proposal ASPE [57]

the methods reported in [63, 66, 76, 88] for Barbara and Mandrill images in terms of PSNR and payload (bpp: bits per pixel). As shown in the figure, the proposed scheme provides high enough bound of the PSNR (above 40dB) with a quite large data embedding capacity, indicating fairly better performance of this method.

3.3 Reversible and high-capacity data hiding in medical images

Data hiding is the insertion of a message, also called content, watermark or embedded message, into a host document or cover media. It is required that the embedded information remains hidden to any unauthorised user. Non-interfering with the marked document and its integrity and authentication to any attempt to suppress it are also key requirements [89]. Not only does the data hiding system have to be reversible, the capacity of the medical file is required to accommodate all information necessary for the doctor such as the identification of the patient, his administrative information and the medical database [90]. Thus, high quality (fidelity), authentication, high capacity, frequent insertions and reversibility are the main requirements of medical files.

In the past two decades, a variety of data hiding schemes that can meet the above requirements have been proposed and applied to medical images. Various kinds of data hiding for medical images that may meet some but not all the requirements can be categorised into three requirements of high quality, reversibility and high capacity.

To preserve high quality, one may embed information in the region of non-interest (RONI) [91, 92]. The main drawback of this method is the ease of

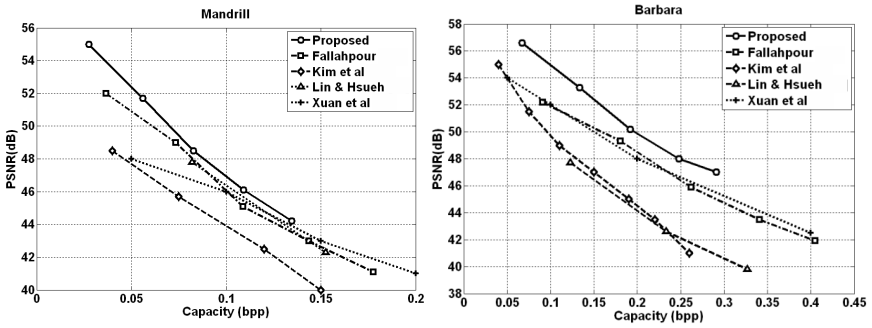


Figure 3.4: Comparison for Mandrill and Barbara images among the reversible methods in Fallahpour [88], Kim et al [76], Lin & Hsueh [63], Xuan et al [66], and our proposal [58]

introducing copy attack on the non-watermarked regions. Various experiments suggest that RONI corresponds in general to the black background of the image, but sometimes RONI can include grey-level parts of little interest [93], thus leaving some area for embedding on the grey-level image itself. As there is no interference with the invisibility, image content is less strict; consequently, one can revert to methods with higher robustness and capacity [91]. Another medical image watermarking system embeds information in bit planes, which results in stego images with very low normalised root mean-squared errors (NRMSE), indicating that the watermark is practically invisible [94]. A watermark that is embedded in the highfrequency regions of an image has also been proposed, which also resulted in low NRMSEs [94].

On the reversible data hiding, where the embedded content can be added or removed without affecting the original image quality, [95], a vast attempt has recently been provided. However, the capacity is still way below the embedding capacity of the non-reversible data hiding technique. However, if capacity is of prime importance, then quality can be sacrificed for capacity. For instance, the embedded data may replace some image details such as the least significant bit of the image [96] or details are lost after lossy image compression [97]. For a survey on medical watermarking application, the readers may refer to [98].

Perhaps the histogram-shifted-based lossless data hiding algorithm proposed by Ni et al. [79] is one of the most capacity-efficient data hiding system that suits medical images well. As in this method, at most the intensity of all the watermarked pixels are shifted by one quantum level, then for an 8-bit image with the mean-squared error (MSE) of 1, the PSNR of the watermarked image, at worst is $\text{PSNR} = 10 \times \text{Log}_{10}(255 \times 255/\text{MSE}) = 48.13$ dB, which is regarded a very high quality and is suitable for medical images. Recently, Lin et al. [99] suggested a high-capacity and low-distortion algorithm based on differences between the neighbouring pixels. Tsai et al. [84] with a predictive coding algorithm propose a technique that improves Ni et al. [79] for some images by about 1.5

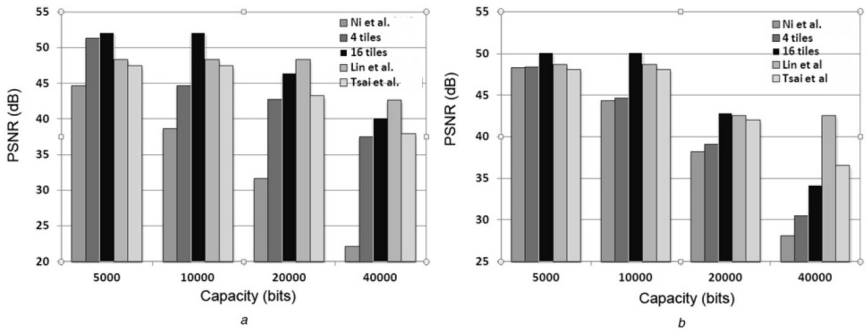


Figure 3.5: Comparison among Ni et al. [79], Lin et al [99], Tsai et al. [84] and our proposal [60] with 4 and 16 tiles.

dB. However, the performance of their method is image content dependent and for some images at the same capacity, the quality is poorer than [79].

In [60], we show how by applying shifted-histogram on the tiled images, not only the watermarked image quality can be improved, but more importantly, the data hiding payload can be significantly increased. Other advantages of the proposed system include data hiding on the RONIs and capacity-quality trade-off.

We have implemented and compared the performance of algorithms in [79, 99, 84] with our proposed method [60] (for 4 and 16 image tiles) on a variety of medical images. The original image sizes were 512 512 pixels with 8 bit resolution.

Fig. 3.5 compares the performance of Ni et al. [79], Lin et al. [99] and Tsai et al. [84] against our proposal [60] (for 4 and 16 tiles) in terms of capacity and PSNR for the two extreme images of Im 5 and Im 10. For Im 5, at low capacity of up to 10 kbits, our method with a 16-tile image is the best, but for capacity larger than 20 kbits method [99] is better. For Im 10, our 16-tile version outperforms all up to 20kbits data hiding capacity and is inferior to [99, 84] at 40 kbits. Our method with the ability of RONI, can result in a better subjective picture quality, than all these methods which are applied to the whole image.

Chapter 4

Watermarking of remote sensing images

This chapter presents the related work on watermarking of remote sensing images. The only section of this chapter summarizes the work on the following papers:

[100] J. Serra-Ruiz and D. Megías, "Watermarking scheme for tampering detection in remote sensing images using variable size tiling and DWT," in *Proceedings of Satellite Data Compression, Communications, and Processing VI* (B. Huang, A. Plaza, J. Serra-Sagrista, C. Lee, Y. Li, and S. Qian, eds.), vol. 7810, (San Diego), p. 78100A, SPIE, August 2010.

[101] J. Serra-Ruiz and D. Megías, "DWT and TSVQ-based semi-fragile watermarking scheme for tampering detection in remote sensing images," in *Image and Video Technology (PSIVT), 2010 Fourth Pacific-Rim Symposium on*, pp. 331–336, November 2010.

[102] J. Serra-Ruiz and D. Megías, "A novel semi-fragile forensic watermarking scheme for remote sensing images," *International Journal of Remote Sensing*, vol. 19, pp. 5583–5606, 2011.

[103] J. Serra-Ruiz and D. Megías, "Reversible data hiding for tampering detection in remote sensing images using histogram shifting," pp. 85140Y–85140Y–11, 2012.

4.1 Watermarking of remote sensing images

Remote Sensing images have gained increased attention by the research community in recent years, since new uses and applications of this area are often reported. Looking for water in remote planets (NASA missions), water pollution control, high precision farming or natural resources management, among others,

are well-known uses of these images [104, 105]. The acquisition of remote sensing images involves expensive equipment like aircraft or satellites. Therefore their economic value must be preserved when a third party pays for them.

To prevent illegal copies and the alteration of digital files (audio or image), some methods and techniques have been developed to embed a watermark into the digital files. This watermark must be imperceptible and can used to determine the integrity of the digital files. In this authentication process, two different approaches, namely semi-fragile watermarking and robust watermarking, can be used.

Semi-fragile watermarking makes unnecessary the marking of different versions of the same image independently and, thus, reduces the cost required to distribute different versions of the same image with different degrees of quality. If the client has access to a compressed version of the image, he or she may check the integrity of the image (discarding tampering). After that, he or she may be interested in getting access to the original uncompressed image at a higher price. For example, the schemes [106, 107] embed a watermark into an image in such a way that the embedded information is destroyed or modified if the image is tampered. It is modified or destroyed when the marked image is manipulated.

Robust watermarking methods are those for which the mark is detected after strong alterations. Robust watermarking schemes have proven successful in order to protect images in several ways, such as resolving authoring disputes or detecting changes in the images aimed to produce a forged copy, as shown in [108, 109].

In remote sensing imaging applications, the most useful schemes aimed to detect changes in the image are semi-fragile watermarking systems. There are previous works dealing with satellite image watermarking [110, 111, 112, 113, 114]. [111] use a satellite image and decompose it into two mutually orthogonal subfields, but only uses one band of the satellite image and only one field for watermarking purposes. [110] present a semi-fragile watermarking scheme based on wavelet transforms. The edge and texture of the remote sensing image are extracted and the watermark is embedded only in the edge character. In this case, once again, only one band is marked. [113] present a scheme to embed an authentication mark using the method described by [107] to mark and compress the image at the same time. This scheme uses only one band to embed the mark into each block to detect manipulations. [112] present a watermarking scheme to preserve a digital content, but only uses one band of the hyperspectral image of the Indian Remote Sensing System. Finally, [114] describe an evolutionary algorithm which marks an image based on the manipulation of the discrete cosine transform (DCT) computed for each band of the image. [115] describe a method to embed one mark into the hyperspectral image using the whole signature, but it does not allow compression of the hyperspectral image. This adaptive watermarking method based on the redundant discrete wavelet transform (RDWT) is a fragile scheme.

In [100] and [101], an optional preliminary step, with near-lossless compression and decompression can be aapplied to the image in order to eliminate

possible sensors errors. Firstly, the original multispectral or hyperspectral image is segmented in three-dimensional blocks using a tiling process with different blocks sizes. Secondly, an integer discrete Wavelet transform (DWT) is applied for each block.

Usually, fragile or semi-fragile watermarking schemes of multiple band images also consider only one band or process each band separately [116, 113]. It is possible to work with images using only one band for computing where and how to embed the watermark, but then, when multiband images are marked with the same method, the bands are usually marked separately or only one band or a subset of bands are marked. Note that, if the bands are marked separately, the changes in the signature curves can be uneven (some values can be increased and others decreased, for the same pixel). Hence, the shapes of the signatures may vary, which may lead to a misclassification of the image (for example, a different material could be identified in the image). Because of this, a method which preserves the shapes of the signatures is highly demanded, and this can be achieved by working with the signatures as a whole.

The method we suggest in [102] uses the hyperspectral image as a whole applying a vector quantization approach. The image is segmented in three-dimensional blocks of a given size which determines the spatial resolution of the embedding and detection algorithm. For each block, a tree with an endmember (real values read by the sensor for each pixel region) of the remote sensing image is built and these endmembers are manipulated by removing the least significant bits in order to increase the robustness against possible near-lossless compression attacks. Finally, the block is manipulated using an iterative algorithm until the resulting block (TSVQ tree) satisfies some criterion. The image is modified according to a secret key which produces a different criterion for each block in order to avoid copy-and-replace attacks. This key determines the internal structure of the tree and also the resulting distortion.

Some previous works have been selected and compared with our proposed method [102]. All of them are blind–except [115]–, semi-fragile and allow some level of compression. The selected method can be used for tampering detection, but not all of them report the tamper localization.

Table 4.1 shows the results obtained with each method. In the first column, the chosen method is referenced. The second column shows the type of the remote sensing image used in the corresponding method. The third column describes whether the method is applied to a single band, a subset of bands or the whole signature. The fourth column reports the PSNR obtained with each method (if available). Finally, the fifth column indicates whether the method can be used for tamper localization, reporting either the size of the identified tampered area or "No" if it can applied only for tamper detection (not localization).

Among the methods which are applied to hyperspectral images, note that [114] is applied to each band separately, which means that the signature is not modified evenly and the curve can be significantly altered. The scheme described by [114] can be used to detect tampering, but not the localization of manipulated signatures. Finally, although the scheme of [115] works with the whole signature

Table 4.1: Comparison of watermarking systems and our proposal [102].

Scheme	Image type	Embedding strategy	PSNR	Tamper localization
[113]	Greyscale (1 band)	1 band	$\leq$ 45 dB (8 bpp)	16×8 blocks
[111]	Greyscale (1 band)	1 band	$\sim$ 40 dB (8 bpp)	8×8 blocks
[110]	RGB	RGB	Not reported	$\sim$ Tampered area
[112]	Panchromatic (1 band)	1 band	$\sim$ 55 dB (8 bpp)	No
[114]	Hyperspectral	Band by band	Not reported	No
[115]	Hyperspectral	Selected signatures	Not reported	No
[102]	**Hyperspectral**	**16 bands**	$\sim$ 80 **dB (14 bpp)** $\sim$ 70 **dB (8 bpp)**	64×64 **(or** 32×32**)**

of a set of pixels, it does not provide information about tamper localization either. As the size of the tampering localization is concerned, [110, 111, 113] make it possible to identify smaller tampered areas compared to the proposed scheme, but those methods must be applied to each separate band and yield worse PSNR results.

Some of the reversible watermarking schemes apply transformations directly to the pixel values. The first few works applying these techniques were Refs. [64] and [117] , which use the idea of difference expansion, or Ref. [118], which presents an algorithm based on an integer transformation of four adjacent pixels.

A different family of reversible watermarking schemes is based on the interpolation of the pixel values. In this type of algorithms, some pixel values are interpolated based on their neighboring pixels [119]. The watermark bitstream is added to the interpolation error introduced in the first interpolation. The interpolation and the watermark are combined to create the marked image. In the extraction scheme, the marked pixels are interpolated, and their values determine the interpolation errors. Then, the watermark is removed from the errors and the result is combined with the interpolated pixels to restore the original image.

Another strategy for reversible watermarking is based on data compression. The main idea of this class of algorithms is to compress some of the bit planes of the image losslessly to produce additional space for embedding the watermark. This is applied to the least significant bit planes, such that the distortion is as low as possible. The method proposed in Ref. [74] applies quantization to each pixel and obtains the quantized value and the remainder. These remainders are losslessly compressed and appended to the watermark bits. Finally, the

resulting values are converted to L-ary symbols, with L being the quantization level, and added to the quantized pixel values to obtain the marked image. In the extraction scheme, the marked pixels are quantized with the level L, the watermark bitstream is extracted from these quantized pixels, and the leftover portion of the result is decompressed to recover the quantization remainders. Finally, the quantized pixel values of the first step and the retrieved remainders are added to restore the original image.

Histogram shifting is another strategy used in reversible watermarking. The main idea of this technique is the use of the frequency distribution of the pixel values of an image, usually grayscale, to hide the watermark bitstream. The method proposed by Ni *et al.* [79] determines the peak value of the image histogram and all values greater than the peak value in the histogram are shifted one bin to the right, *i.e.* are incremented by one unit. This produces an empty bin just next to the histogram's peak.

The final type of reversible watermarking schemes is based on modifying some frequency-domain coefficients. Yang *et al.* [120] present a method using this type of strategy. The image is segmented into blocks of 8×8 pixels and the integer DCT is applied. Some coefficients of the DCT are shifted in order to embed the watermark in the LSB positions. Finally, the inverse integer DCT is calculated to these coefficient blocks to produce the marked image. In the extraction scheme, the marked image is segmented into the same 8×8 blocks and the integer DCT is applied. Then, the LSBs of the selected DCT coefficients are extracted. Thus, the watermark bitstream is obtained by joining the extracted LSBs. Finally, the inverse integer DCT is applied to the LSB-extracted and right-shifted DCT coefficients embedded in the image.

All the reported reversible watermarking schemes are designed for grayscale images and cannot be directly applied to hyperspectral images. In remote sensing images, a pixel is formed by a vector of samples and not scalar values, as occurs in grayscale images. The most obvious possibility is to apply these methods to each separate band of a multiband image, but this would produce uneven alterations in the signature curves. A better option is to extend some of these methods to work with vectorial instead of scalar data. In [103], the histogram shifting strategy is applied and generalized to consider hyperspectral images. The image is segmented into smaller blocks of pixels (or endmembers) which are vectorial data. The histogram is constructed for the maximum component of the vectorial values of the pixels (*i.e.* the infinity norm) in each block, and this histogram is shifted in order to leave an empty gap which is used by the scheme to embed the authentication information. The suggested method is still reversible, making it possible to recover the original image in the extraction-authentication process. In addition, the block-based implementation of the scheme makes it possible to locate specific tampered areas of the image. The only drawback of the proposed method is fragility, since it does not allow any change of the marked image, including near lossless compression.

Unlike [100, 101, 102], note that this process is fragile and no changes to the marked images are allowed (not even a near lossless compression). If near lossless compression must be allowed, the scheme should be modified to be semi-fragile.

Bibliography

[1] D. Megías, J. Serra-Ruiz, and M. Fallahpour, "Efficient self-synchronised blind audio watermarking system based on time domain and FFT amplitude modification," *Signal Process.*, vol. 90, pp. 3078–3092, Dec. 2010. *

[2] M. Fallahpour and D. Megías, "DWT-based high capacity audio watermarking," *IEICE Transactions*, vol. 93-A, no. 1, pp. 331–335, 2010. *

[3] M. Fallahpour and D. Megías, "High capacity audio watermarking using the high frequency band of the wavelet domain," *Multimedia Tools Appl.*, vol. 52, pp. 485–498, Apr. 2011. *

[4] M. Fallahpour and D. Megías, "High capacity method for real-time audio data hiding using the FFT transform," *Advances in Information Security and Its Applications*, vol. 36, pp. 91–97, 2009. *

[5] M. Fallahpour and D. Megías, "Robust high-capacity audio watermarking based on FFT amplitude modification," *IEICE Transactions*, vol. 93-D, no. 1, pp. 87–93, 2010. *

[6] M. Fallahpour and D. Megías, "High capacity FFT-based audio watermarking," in *Proceedings of the 12th IFIP TC 6/TC 11 international conference on Communications and multimedia security*, CMS'11, (Berlin, Heidelberg), pp. 235–237, Springer-Verlag, 2011. *

[7] M. Fallahpour and D. Megías, "High capacity logarithmic audio watermarking based on the human auditory system," in *Proceedings IEEE International Symposium on Multimedia*, ISM2012, 2012. *

[8] I.-K. Yeo and H. J. Kim, "Modified patchwork algorithm: a novel audio watermarking scheme," *Speech and Audio Processing, IEEE Transactions on*, vol. 11, pp. 381 – 386, july 2003.

[9] S. Xiang, H. J. Kim, and J. Huang, "Audio watermarking robust against time-scale modification and mp3 compression," *Signal Process.*, vol. 88, pp. 2372–2387, Oct. 2008.

[10] M. Fan and H. Wang, "Chaos-based discrete fractional sine transform domain audio watermarking scheme," *Comput. Electr. Eng.*, vol. 35, pp. 506–516, May 2009.

[11] H. Kang, K. Yamaguchi, B. Kurkoski, K. Yamaguchi, and K. Kobayashi, "Full-index-embedding patchwork algorithm for audio watermarking," *IEICE - Trans. Inf. Syst.*, vol. E91-D, pp. 2731–2734, Nov. 2008.

[12] Y. Lin and W. Abdulla, "A secure and robust audio watermarking scheme using multiple scrambling and adaptive synchronization," in *Proceedings of the 6th International Conference on Information, Communications and Signal Processing*, pp. 1–5, 2007.

[13] S. Sun and S. Kwong, "A self-synchronization blind audio watermarking algorithm," in *Intelligent Signal Processing and Communication Systems, 2005. ISPACS 2005. Proceedings of 2005 International Symposium on*, pp. 133 – 136, dec. 2005.

[14] Z. Liu and A. Inoue, "Audio watermarking techniques using sinusoidal patterns based on pseudorandom sequences," *Circuits and Systems for Video Technology, IEEE Transactions on*, vol. 13, pp. 801 – 812, aug. 2003.

[15] L. Hai-yan, Z. Xue-feng, and W. Ying, "DWT-based audio watermarking resistant to desynchronization," in *Computer and Information Technology, 2007. CIT 2007. 7th IEEE International Conference on*, pp. 745 –748, oct. 2007.

[16] H. Wang, Y. Sun, L. Lu, and W. Shu, "Anti-cropping synchronization audio digital watermark algorithm based on watermark sequence number," in *Signal Processing, 2006 8th International Conference on*, vol. 4, 16-20 2006.

[17] Z. Li, C. Li-min, and Q. Gong-bin, "Self-synchronization adaptive blind audio watermarking," in *Multi-Media Modelling Conference Proceedings, 2006 12th International*, p. 4 pp., 0-0 2006.

[18] S. Wu, J. Huang, D. Huang, and Y. Shi, "Efficiently self-synchronized audio watermarking for assured audio data transmission," *Broadcasting, IEEE Transactions on*, vol. 51, pp. 69 – 76, march 2005.

[19] J. Huang, Y. Wang, and Y. Shi, "A blind audio watermarking algorithm with self-synchronization," in *Circuits and Systems, 2002. ISCAS 2002. IEEE International Symposium on*, vol. 3, pp. 627 –630, 2002.

[20] X.-Y. Wang and H. Zhao, "A novel synchronization invariant audio watermarking scheme based on DWT and DCT," *Signal Processing, IEEE Transactions on*, vol. 54, pp. 4835 –4840, dec. 2006.

[21] D. Megías, J. Herrera-Joancomartí, and J. Minguillón, "A robust audio watermarking scheme based on mpeg 1 layer 3 compression," in *Communications and Multimedia Security* (A. Lioy and D. Mazzocchi, eds.), vol. 2828 of *Lecture Notes in Computer Science*, pp. 226–238, Springer, 2003.

[22] D. Megías, J. Herrera-Joancomartí, and J. Minguillón, "Total disclosure of the embedding and detection algorithms for a secure digital watermarking scheme for audio," in *Proceedings of the 7th international conference on Information and Communications Security*, ICICS'05, (Berlin, Heidelberg), pp. 427–440, Springer-Verlag, 2005.

[23] M. Fallahpour and D. Megías, "High capacity audio watermarking using FFT amplitude interpolation," *IEICE Electron. Express*, vol. 6, no. 14, pp. 1057–1063, 2009.

[24] J. J. Garcia-Hernandez, M. Nakano-Miyatake, and H. Perez-Meana, "Data hiding in audio signal using rational dither modulation," *IEICE Electron. Express*, vol. 5, no. 7, pp. 217–222, 2008.

[25] M. Akhaee, M. Saberian, S. Feizi, and F. Marvasti, "Robust audio data hiding using correlated quantization with histogram-based detector," *Multimedia, IEEE Transactions on*, vol. 11, pp. 834 –842, aug. 2009.

[26] B. Chen and G. Wornell, "Quantization index modulation: a class of provably good methods for digital watermarking and information embedding," in *Information Theory, 2000. Proceedings. IEEE International Symposium on*, p. 46, 2000.

[27] Z. Xu, K. Wang, and X. hua Qiao, "Digital audio watermarking algorithm based on quantizing coefficients," *Intelligent Information Hiding and Multimedia Signal Processing, International Conference on*, vol. 0, pp. 41–46, 2006.

[28] M. Pooyan and A. Delforouzi, "Adaptive and robust audio watermarking in wavelet domain," in *Intelligent Information Hiding and Multimedia Signal Processing, 2007. IIHMSP 2007. Third International Conference on*, vol. 2, pp. 287 –290, nov. 2007.

[29] N. Lie and L. Chang, "Multiple watermarks for stereo audio signals using phase-modulation," *IEEE Trans Signal Processing*, vol. 53, no. 2, pp. 806–815, 2000.

[30] H. J. Kim and Y. H. Choi, "A novel echo-hiding scheme with backward and forward kernels," *Circuits and Systems for Video Technology, IEEE Transactions on*, vol. 13, pp. 885 – 889, aug. 2003.

[31] "Stirmark benchmark for audio." `http://wwwiti.cs.uni-magdeburg.de/~alang/smba.php`. (accessed on June 22nd, 2012).

[32] M. Mansour and A. Tewfik, "Data embedding in audio using time-scale modification," *Speech and Audio Processing, IEEE Transactions on*, vol. 13, pp. 432 – 440, may 2005.

[33] W. Li and X. Xue, "Content based localized robust audio watermarking robust against time scale modification," *IEEE Trans. Multimedia*, vol. 8, no. 1, pp. 60–69, 2006.

[34] S.-K. Lee and Y.-S. Ho, "Digital audio watermarking in the cepstrum domain," *IEEE Trans. on Consum. Electron.*, vol. 46, pp. 744–750, Aug. 2000.

[35] X. Li and H. H. Yu, "Transparent and robust audio data hiding in cepstrum domain," in *IEEE International Conference on Multimedia and Expo (I)*, vol. 1, pp. 397–400, 2000.

[36] S.-C. Liu and S. D. Lin, "BCH code-based robust audio watermarking in the cepstrum domain.," *J. Inf. Sci. Eng.*, vol. 22, no. 3, pp. 535–543, 2006.

[37] C.-T. Hsieh and P.-Y. Sou, "Blind cepstrum domain audio watermarking based on time energy features," in *Digital Signal Processing, 2002. DSP 2002. 2002 14th International Conference on*, vol. 2, pp. 705 – 708 vol.2, 2002.

[38] S. Li, L. Cui, J. Choi, and X. Cui, "An audio copyright protection schemes based on smm in cepstrum domain," in *Proceedings of the 2006 joint IAPR international conference on Structural, Syntactic, and Statistical Pattern Recognition*, SSPR'06/SPR'06, (Berlin, Heidelberg), pp. 923–927, Springer-Verlag, 2006.

[39] H.-T. Hu and W.-H. Chen, "A dual cepstrum-based watermarking scheme with self-synchronization," *Signal Process.*, vol. 92, pp. 1109–1116, Apr. 2012.

[40] B. Ko, R. Nishimura, and Y. Suzuki, "Log-scaling watermark detection in digital audio watermarking," in *Acoustics, Speech, and Signal Processing, 2004. Proceedings. (ICASSP '04). IEEE International Conference on*, vol. 3, pp. iii – 81–4 vol.3, may 2004.

[41] R. Yang, X. Kang, and J. Huang, "Robust audio watermarking based on log-polar frequency index," in *IWDW* (H.-J. Kim, S. Katzenbeisser, and A. T. S. Ho, eds.), vol. 5450 of *Lecture Notes in Computer Science*, pp. 124–138, Springer, 2008.

[42] R. Garcia *et al.*, "Digital watermarking of audio signals using a psychoacoustic auditory model and spread spectrum theory," in *Proc. 107th Conv. Aud. Eng. Soc*, pp. 123–131, 1999.

[43] H.-H. Tsai, J.-S. Cheng, and P.-T. Yu, "Audio watermarking based on has and neural networks in dct domain," *EURASIP Journal on Advances in Signal Processing*, vol. 2003, no. 3, p. 764030, 2003.

[44] M. K. Dutta, P. Gupta, and V. K. Pathak, "A perceptible watermarking algorithm for audio signals," *Multimedia Tools and Applications*, pp. 1–23, 2012.

[45] No, Really, "Rust." `http://www.jamendo.com/en/album/7365`.

[46] A. Nishimura, "Audio data hiding that is robust with respect to aerial transmission and speech codecs," *International Journal of Innovative Computing, Information and Control*, vol. 6, no. 3(B), pp. 1389–1400, 2010.

[47] X. Kang, R. Yang, and J. Huang, "Geometric invariant audio watermarking based on an lcm feature," *Multimedia, IEEE Transactions on*, vol. 13, pp. 181 –190, april 2011.

[48] M. Fallahpour, D. Megías, and H. Najaf-Zadeh, "Adaptive speech watermarking in wavelet domain based on logarithm," in *SECRYPT*, pp. 412–415, 2012. *

[49] A. Sagi and D. Malah, "Bandwidth extension of telephone speech aided by data embedding," *EURASIP J. Appl. Signal Process.*, vol. 2007, pp. 37–37, Jan. 2007.

[50] S. Chen and H. Leung, "Speech bandwidth extension by data hiding and phonetic classification," in *Acoustics, Speech and Signal Processing, 2007. ICASSP 2007. IEEE International Conference on*, vol. 4, pp. IV–593 – IV–596, april 2007.

[51] M. Celik, G. Sharma, and A. Murat Tekalp, "Pitch and duration modification for speech watermarking," in *Acoustics, Speech, and Signal Processing, 2005. Proceedings. (ICASSP '05). IEEE International Conference on*, vol. 2, pp. 17 – 20, 18-23, 2005.

[52] "Itu-t, recommendation p.723." `http://www.itu.int/rec/TREC-P.723/en`. (accessed on June 22nd, 2012).

[53] Y. Hu and P. C. Loizou, "Subjective comparison and evaluation of speech enhancement algorithms," *Speech Commun.*, vol. 49, pp. 588–601, July 2007.

[54] A. Gurijala and J. R. Deller, Jr., "On the robustness of parametric watermarking of speech," in *Proceedings of the 2007 international conference on Multimedia content analysis and mining*, MCAM'07, (Berlin, Heidelberg), pp. 501–510, Springer-Verlag, 2007.

[55] L. Girin and S. Marchand, "Watermarking of Speech Signals Using the Sinusoidal Model and Frequency Modulation of the Partials," in *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP04)*, (Montreal, Quebec, Canada), Institute of Electrical and Electronics Engineers (IEEE), May 2004.

[56] M. Fallahpour and D. Megías, "Digital watermarking," ch. Reversible Data Hiding Based On H.264/AVC Intra Prediction, pp. 52–60, Berlin, Heidelberg: Springer-Verlag, 2009. *

[57] M. Fallahpour, D. Megías, and M. Ghanbari, "Subjectively adapted high capacity lossless image data hiding based on prediction errors," *Multimedia Tools Appl.*, vol. 52, no. 2-3, pp. 513–527, 2011. *

[58] M. Fallahpour, D. Megías, and Y. Q. Shi, "Lossless image data embedding in plain areas ," pp. 78800H–78800H–8, 2011. *

[59] M. Fallahpour, D. Megías, and M. Ghanbari, "High capacity, reversible data hiding in medical images," in *Proceedings of the 16th IEEE international conference on Image processing*, ICIP'09, (Piscataway, NJ, USA), pp. 4185–4188, IEEE Press, 2009. *

[60] M. Fallahpour, D. Megías, and M. Ghanbari, "Reversible and high-capacity data hiding in medical images," *Image Processing, IET*, vol. 5, pp. 190 –197, march 2011. *

[61] I.-T. R. H. 14496-10, "Advanced video coding," Mar. 2003. Final Committee Draft, Document JVTG050.

[62] Y. Q. Shi, Z. Ni, D. Zou, C. Liang, and G. Xuan, "Lossless data hiding: fundamentals, algorithms and applications," in *ISCAS (2)*, pp. 33–36, 2004.

[63] C.-C. Lin and N.-L. Hsueh, "Hiding data reversibly in an image via increasing differences between two neighboring pixels," *IEICE - Trans. Inf. Syst.*, vol. E90-D, pp. 2053–2059, Dec. 2007.

[64] J. Tian, "Reversible data embedding using a difference expansion," *IEEE Trans. Circuits Syst. Video Techn.*, vol. 13, no. 8, pp. 890–896, 2003.

[65] L. Kamstra and H. J. Heijmans, "Reversible data embedding into images using wavelet techniques and sorting," *Trans. Img. Proc.*, vol. 14, pp. 2082–2090, Dec. 2005.

[66] G. Xuan, Y. Q. Shi, P. Chai, X. Cui, Z. Ni, and X. Tong, "Optimum histogram pair based image lossless data embedding," in *IWDW* (Y. Q. Shi, H.-J. Kim, and S. Katzenbeisser, eds.), vol. 5041 of *Lecture Notes in Computer Science*, pp. 264–278, Springer, 2007.

[67] G. Xuan, Y. Q. Shi, C. Yang, Y. Zhen, D. Zou, and P. Chai, "Lossless data hiding using integer wavelet transform and threshold embedding technique," in *ICME*, pp. 1520–1523, IEEE, 2005.

[68] D. M. Thodi and J. J. Rodríguez, "Expansion embedding techniques for reversible watermarking," *IEEE Transactions on Image Processing*, vol. 16, no. 3, pp. 721–730, 2007.

[69] M. Kuribayashi, M. Morii, and H. Tanaka, "Reversible watermark with large capacity based on the prediction error expansion," *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, vol. E91-A, pp. 1780–1790, July 2008.

[70] M. Fallahpour and M. Sedaaghi, "High capacity lossless data hiding based on histogram modification," *IEICE Transactions on Electronics Express*, vol. 4, no. 7, pp. 205–210, 2007.

[71] "Waterloo repertoire greyset2." `http://links.uwaterloo.ca/greyset2.base.html`. Last checked on October 27th, 2008.

[72] J.-B. Feng, I.-C. Lin, C.-S. Tsai, and Y.-P. Chu, "Reversible watermarking: Current status and key issues," *I. J. Network Security*, vol. 2, no. 3, pp. 161–170, 2006.

[73] J. Fridrich, M. Goljan, and R. Du, "Invertible authentication," in *Proceedings of SPIE Photonics West*, vol. 3971 of *Security and Watermarking of Multimedia Contents III*, pp. 197–208, January 2001.

[74] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Lossless generalized-LSB data embedding," *IEEE Transactions on Image Processing*, vol. 14, no. 2, pp. 253–266, 2005.

[75] A. M. Alattar, "Reversible watermark using the difference expansion of a generalized integer transform," *IEEE Transactions on Image Processing*, vol. 13, no. 8, pp. 1147–1156, 2004.

[76] H. J. Kim, V. Sachnev, Y. Q. Shi, J. Nam, and H.-G. Choo, "A novel difference expansion transform for reversible data embedding," *Trans. Info. For. Sec.*, vol. 3, pp. 456–465, Sept. 2008.

[77] C.-C. Chang, W.-L. Tai, and C.-C. Lin, "A reversible data hiding scheme based on side match vector quantization," *IEEE Trans. Cir. and Sys. for Video Technol.*, vol. 16, pp. 1301–1308, Oct. 2006.

[78] C.-C. Chang and C.-Y. Lin, "Reversible steganography for vq-compressed images using side matching and relocation," *IEEE Transactions on Information Forensics and Security*, vol. 1, no. 4, pp. 493–501, 2006.

[79] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," *IEEE Trans. Circuits Syst. Video Techn.*, vol. 16, no. 3, pp. 354–362, 2006.

[80] X. Gao, L. An, X. Li, and D. Tao, "Reversibility improved lossless data hiding," *Signal Process.*, vol. 89, pp. 2053–2065, Oct. 2009.

[81] J. Hwang, J. Kim, and J. Choi, "A reversible watermarking based on histogram shifting," in *Proceedings of the 5th international conference on Digital Watermarking*, IWDW'06, (Berlin, Heidelberg), pp. 348–361, Springer-Verlag, 2006.

[82] K.-S. Kim, M.-J. Lee, H.-K. Lee, and Y.-H. Suh, "Histogram-based reversible data hiding technique using subsampling," in *Proceedings of the 10th ACM workshop on Multimedia and security*, MM&Sec '08, (New York, NY, USA), pp. 69–74, ACM, 2008.

[83] W. Hong, T.-S. Chen, and C.-W. Shiu, "Reversible data hiding based on histogram shifting of prediction errors," in *Proceedings of the 2008 International Symposium on Intelligent Information Technology Application Workshops*, IITAW '08, (Washington, DC, USA), pp. 292–295, IEEE Computer Society, 2008.

[84] P. Tsai, Y.-C. Hu, and H.-L. Yeh, "Reversible image hiding scheme using predictive coding and histogram shifting," *Signal Process.*, vol. 89, pp. 1129–1143, June 2009.

[85] M. J. Weinberger, G. Seroussi, and G. Sapiro, "The LOCO-I lossless image compression algorithm: principles and standardization into JPEG-LS," *IEEE Transactions on Image Processing*, vol. 9, no. 8, pp. 1309–1324, 2000.

[86] X. Wu and N. D. Memon, "Context-based, adaptive, lossless image coding.," *IEEE Transactions on Communications*, vol. 45, no. 4, pp. 437–444, 1997.

[87] J. Jiang, B. Guo, and S. Y. Yang, "Revisiting the JPEG-LS prediction scheme," *Vision, Image and Signal Processing*, pp. 575–580, 2000.

[88] M. Fallahpour, "Reversible image data hiding based on gradient adjusted prediction," *IEICE Electron. Express*, vol. 5, no. 20, pp. 870–876, 2008.

[89] E. J. Delp, "Multimedia security: the 22nd century approach," *Multimedia Syst.*, vol. 11, no. 2, pp. 95–97, 2005.

[90] U. Rajendra Acharya, D. Acharya, P. Subbanna Bhat, and U. C. Niranjan, "Compact storage of medical images with patient information," *Trans. Info. Tech. Biomed.*, vol. 5, pp. 320–323, Dec. 2001.

[91] C. G, S. B, and M. H, "Strict integrity control of biomedical images," *Proc. Security and Watermarking of Multimedia Contents III*, pp. 229 – 240, 2001.

[92] A. Wakatani, "Digital watermaking for roi medical images by using compresses signature image," in *Proceedings of the 35th Annual Hawaii International Conference on System Sciences (HICSS'02)-Volume 6 - Volume 6*, HICSS '02, (Washington, DC, USA), pp. 157–, IEEE Computer Society, 2002.

[93] F. Y. Shih and Y.-T. Wu, "Robust watermarking and compression for medical images based on genetic algorithms," *Inf. Sci.*, vol. 175, pp. 200–216, Oct. 2005.

[94] J. Nayak, P. S. Bhat, R. Acharya U, and N. UC, "Simultaneous storage of medical images in the spatial and frequency domain: A comparative study," *BioMedical Engineering OnLine*, vol. 3, no. 1, p. 17, 2004.

[95] B. Macq and D. F., "Trusted headers for medical images," in *DFG VIII-DII Watermarking Workshop*, (Germany), 1999.

[96] X. Zhou, H. K. Huang, and S.-L. Lou, "Authenticity and integrity of digital mammography images," *IEEE Trans. Med. Imaging*, vol. 20, no. 8, pp. 784–791, 2001.

[97] M. Li, R. Poovendran, and S. Narayanan, "Protecting patient privacy against unauthorized release of medical images in a group communication environment," *Computerized Medical Imaging and Graphics*, vol. 29, no. 5, pp. 367 – 383, 2005.

[98] G. Coatrieux, L. Lecornu, B. Sankur, and C. Roux, "A review of image watermarking applications in healthcare," in *Engineering in Medicine and Biology Society, 2006. EMBS '06. 28th Annual International Conference of the IEEE*, pp. 4691 –4694, 30 2006-sept. 3 2006.

[99] C.-C. Lin, W.-L. Tai, and C.-C. Chang, "Multilevel reversible data hiding based on histogram modification of difference images," *Pattern Recogn.*, vol. 41, pp. 3582–3591, Dec. 2008.

[100] J. Serra-Ruiz and D. Megías, "Watermarking scheme for tampering detection in remote sensing images using variablesize tiling and DWT," in *Proceedings of Satellite Data Compression, Communications, and Processing VI* (B. Huang, A. Plaza, J. Serra-Sagrista, C. Lee, Y. Li, and S. Qian, eds.), vol. 7810, (San Diego), p. 78100A, SPIE, August 2010. *

[101] J. Serra-Ruiz and D. Megías, "DWT and TSVQ-based semi-fragile watermarking scheme for tampering detection in remote sensing images," in *Image and Video Technology (PSIVT), 2010 Fourth Pacific-Rim Symposium on*, pp. 331–336, November 2010. *

[102] J. Serra-Ruiz and D. Megías, "A novel semi-fragile forensic watermarking scheme for remote sensing images," *International Journal of Remote Sensing*, vol. 19, pp. 5583–5606, 2011. *

[103] J. Serra-Ruiz and D. Megías, "Reversible data hiding for tampering detection in remote sensing images using histogram shifting," pp. 85140Y–85140Y–11, 2012. *

[104] P. M. Atkinson and N. J. Tate, *Advances in remote sensing and GIS analysis*. Wiley, 1999.

[105] F. C. Wong and N. Y. Lao, "Economic value of remote sensing imagery for agricultural applications," in *Proceedings of the Aerospace Conference*, vol. 8, pp. 3815–3829, March 2003.

[106] M. Yeung and F. Mintzer, "An invisible watermarking technique for image verification," in *International Conference on Image Processing, IEEE*, vol. 2, (Santa Barbara, CA), pp. 680–683, October 1997.

[107] J. Fridrich, "Security of fragile authentication watermarks with localization," *Society of Photo-Optical Instrumentation Engineers (SPIE) Conference Series*, vol. 4675, pp. 691–700, April 2002.

[108] E. Lin, C. Podilchuk, and E. Delp, "Detection of image alterations using semi-fragile watermarks," *Proceedings of the SPIE International Conference on Security and Watermarking of Multimedia Contents II*, vol. 3971, January 2000.

[109] J. Minguillón, J. Herrera-Joancomartí, D. Megías, and J. Serra-Sagristá, "Evaluation of copyright protection schemes for hyperspectral imaging," in *Proceedings of Image and signal processing for remote sensing IX*, vol. 5238, (Barcelona, Spain), pp. 512–523, September 2003.

[110] Q. Qin, W. Wang, and S. Chen, "Research of digital semi-fragile watermarking of remote sensing image based on wavelet analysis," *IEEE International Geoscience and Remote Sensing Symposium*, vol. 1-7, 2004.

[111] A. T. S. Ho, X. Zhu, and W. Woon, "A semi-fragile pinned sine transform watermarking system for content authentication of satellite images," *IEEE International Geoscience and Remote Sensing Symposium*, vol. 1-8, 2005.

[112] X. Wang, Z. Guan, and C. Wu, *Advanced Data Mining and Applications*, vol. 3584/2005 of *LNCS*, ch. A Novel Information Hiding Technique for Remote Sensing Image, pp. 423–430. 2005.

[113] R. Caldelli, F. Filippini, and M. Barni, "Joint near-lossless compression and watermarking of still images for authentication and tamper localization," *Signal Processing: Image Communication*, vol. 21:10, no. 10, pp. 890–903, 2006.

[114] D. Sal and M. Graña, *Studies in Computational Intelligence*, vol. 133/2008, ch. A Multiobjective Evolutionary Algorithm for Hyperspectral Image Watermarking, pp. 63–78. Springer Berlin / Heidelberg, 2008.

[115] H. Tamhankar, L. Bruce, and N. Younan, "Watermarking of hyperspectral data," *Geoscience and Remote Sensing Symposium, 2003. IGARSS '03. Proceedings. 2003 IEEE International*, vol. 6, pp. 3574–3576 vol.6, July 2003.

[116] O. Ekici, B. Sankur, U. Naci, B. Coskun, and M. Akcay, "Comparative assessment of semifragile watermarking methods," *Journal of Electronic Imaging*, vol. 13, pp. 209–216, January 2004.

[117] J. Tian, "Reversible watermarking by difference expansion," in *Proceedings of Workshop on Multimedia and Security*, pp. 19–22, December 2002.

[118] S. Weng, Y. Zhao, J. Pan, and R. Ni, "A novel reversible watermarking based on an integer transform," in *Proceedings of International Conference on Image Processing*, pp. 241–244, September 2007.

[119] L. Luo, Z. Chen, M. Chen, X. Zeng, and Z. Xiong, "Reversible image watermarking using interpolation technique," *IEEE Transactions on Information Forensics and Security*, vol. 5, pp. 187–193, March 2010.

[120] B. Yang, M. Schmucker, W. Funk, C. Busch, and S. Sun, "Integer DCT-based reversible watermarking technique for images using companding technique," in *Proceedings of SPIE*, vol. 5306, pp. 405–415, 2004.