ARES project
CONSOLIDER-INGENIO 2010 CSD2007-00004
Workpackage 3 - Task 4 (WP3.T4)
Audio watermarking
Deliverable Report

David Megías*, Marcel Fernández†, Jordi Herrera-Joancomartí*,‡

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

†Universitat Politècnica de Catalunya,
Departament d'Enginyeria Telemàtica,
Campus Nord, C3 building,
Jordi Girona, 1-3, 08034 Barcelona, Spain
e-mail marcel@entel.upc.edu

‡Universitat Autònoma de Barcelona,
Departament d'Enginyeria de la Informació i de les Comunicacions,
Edifici Q ,08193 Bellaterra - Cerdanyola del Vallès (Barcelona), Spain
e-mail jordi.herrera@uab.cat

October 7, 2009

Contents

Abstract

This report summarises the advances carried out in audio watermarking and other related fields within the ARES project. Firstly, the audio watermarking techniques developed by the ARES team are summarised, and their capacity, transparency, robustness and security properties are highlighted. Secondly, the contribution of the team to the closely related fields of fingerprinting and steganography are described. These methods go one step forward in copy detection, as they make it possible to trace malicious buyers who try to erase the embedded copyright protection information in multimedia files. Finally, some related results in the image field are summarised. These methods have been specifically designed to deal with sensitive information (such as remote sensing or medical images).

Chapter 1

Introduction

The fast growth of the Internet and the digital information revolution is causing significant changes in the global society, ranging from the influence on the world financial system to the way people communicate nowadays. Broadband communication networks and multimedia data existing in a digital format (images, audio and video) have opened many challenges and prospects for innovation. Flexible and simple-to-use software and the decreasing prices of digital devices (*e.g.* digital photo cameras, camcorders, portable CD and MP3 players, DVD players, CD and DVD recorders, laptops, PDAs and so on) have made it possible for users from all over the world to produce, edit and exchange multimedia data. Broadband Internet connections and almost an errorless transmission of data make it possible to distribute large multimedia files and make exact digital copies of them. Digital media files do not suffer from any quality loss due to multiple copying processes, as occurs with analogue audio and VHS tapes. The simplicity of content modification and a perfect reproduction in the digital domain have led the protection of intellectual ownership and the prevention of the unauthorised tampering of multimedia data to become an important technological and research issue [1, 2, 3, 4].

Simple protection methods which were based on the data embedded into header bits of the digital file are useless since the header information can be easily removed by a change of data format, which does not affect the fidelity of media.

Encryption of digital multimedia prevents access to the multimedia content to an individual without a suitable decryption key. Thus, content providers get paid for the delivery of perceivable multimedia, and each client who has paid the royalties must be able to decrypt a received file properly. However, once the multimedia content has been decrypted, it can be repeatedly copied and distributed without any obstacles. Current software applications and broadband Internet provide the tools to carry out it quickly and without deep technical knowledge. One of the most recent cases is the hack of the Content Scrambling System for DVDs [5, 6].

It is obvious that the existing security protocols for electronic commerce

secure only the communication channel between the content provider and the user. Digital watermarking has been proposed as a novel, alternative scheme to protect the intellectual property rights and defend digital media from tampering. It involves a procedure of embedding a perceptually transparent digital signature into a host signal, carrying a message about the host signal in order to "mark" its ownership.

Watermarking algorithms were primarily developed for digital images and video sequences [7, 8] and the interest and research in audio watermarking started slightly later [9, 10]. In the past few years, several algorithms for the embedding and extraction of watermarks in audio sequences have been presented. All of the developed algorithms take advantage of the perceptual properties of the Human Auditory System (HAS) in order to add a watermark into a host signal in a perceptually transparent manner. Embedding additional information into audio sequences is a more difficult task than that of images, due to dynamic supremacy of the HAS over Human Visual System [7]. On the other hand, many attacks which are malicious against image watermarking algorithms (*e.g.* geometrical distortions, spatial scaling, etc.) cannot be implemented against audio watermarking schemes, although other specific attacks exist for digital audio contents.

The objective of this project task was to improve the reliability of audio watermarking, focusing on obtaining new audio watermarking schemes that improve the robustness and security properties of the existing ones. The main results of this task are summarised in Chapter 2. Chapter 3 presents some achievements in steganography and fingerprinting which can also applied to audio contents. In Chapter 4, we report some results which have been obtained in the image field (as a result of the synergy between audio and image watermarking). Finally, the most relevant concluding remarks are summarised in Chapter 5.

Chapter 2

Watermarking of audio contents

The following sections present the results we have achieved in the audio watermarking field.

2.1 Methods in the FFT domain

We have developed a very efficient method for audio data hiding which is suitable for real-time applications [11]. The scheme has been implemented taking special care for the efficient usage of the two restricted resources of computer systems: memory space and CPU time. It offers to the industrial user the capability of watermark embedding and detection in time immediately comparable to the real playing time of the original audio file, while the end user/audience does not find any artifacts or delays hearing the watermarked audio file. In the proposed algorithm, the FFT magnitudes of the selected clip which are in a band of frequency between 5 and 15 kHz are slightly distorted and the magnitudes which have a value lower than a chosen threshold are used for embedding. This frequency band is scanned and when a magnitude with the value lower the threshold is found it is increased if the corresponding embedding bit is '1', otherwise the magnitude is not altered. Low complexity is one of the most important properties of this method, making it appropriate for real-time applications. In addition, the suggested scheme is blind since it does not need the original signal for extracting the hidden bits. The experimental results show that the method has a very high capacity (above 5 kbps) and provides robustness against MPEG compression.

The steps of the embedding and extracting processes are summarised below. The embedding steps are as follows:

1. Based on the computation processor (speed and memory) select the length of the segment of the audio file.

2. Calculate the FFT of the audio segment.

3. Select the band of frequencies between 5 kHz and 15 kHz for which the magnitudes are near 1.

4. Using q as a parameter, convert the FFT magnitudes to integer values (multiplying them by q and then rounding).

5. Expanding step: scan all these integer FFT magnitudes in the selected band. If a magnitude is larger than zero then increase it by one. After this step we have no magnitude with the value 1.

6. Embedding step: scan again all integer FFT magnitudes in the selected band. When a zero magnitude is found, if the corresponding embedded bit is '1' add one to the magnitude. Otherwise, the magnitude is not changed. After this step all magnitudes with value zero or one represent an embedded bit.

7. The marked (FFT) signal is achieved by dividing all the magnitudes by q.

8. Finally, use the IFFT to achieve the marked audio segment in the time domain.

The watermark detection is performed by using the FFT transform and the embedding parameters. Since the host audio signal is not required in the detection process, the detector is blind. The detection process can be summarised in the following steps:

1. Calculate the FFT of the marked audio segment.

2. To obtain the scaled FFT magnitudes, multiply them by q.

3. Detection step: scan all the scaled FFT magnitudes in the selected band. If a magnitude with value in the interval $[0, 1/2)$ is found, then the corresponding embedded bit is equal to '0' and the restored magnitude equals to zero. If the magnitude value is in the interval $[1/2, 3/2)$, then the corresponding embedded bit is equal to '1' and the restored magnitude equals to zero.

4. Scan all the scaled FFT magnitudes in the selected band. If a magnitude value is in interval $[k + 1/2, k + 3/2)$, then the restored magnitude equals to k.

5. The restored magnitudes are obtained by dividing them by q.

6. Finally, use the IFFT to achieve the restored audio segment.

The main properties of the suggested scheme are the following:

1. Capacity of 5 kbps (or higher).

2. Remarkable imperceptibility: Objective Difference Grade (ODG) around -1 (not annoying).

3. Robustness against MP3 compression.

The fact that the suggested method is robust against MP3 compression is not very common in data hiding scheme. Since MP3 compression with a bit rate of 128 kbps provides with 12:1 compression ratios, it makes it possible to increase the capacity of the data hiding system by a factor of 12 as measured in bits of embedded data per bit of the marked audio sequence.

In the case of audio watermarking, the properties of robustness and security become relevant and the capacity of the scheme is not the highest priority. Hence, it is required that the embedded bits are preserved even in the presence of intentional or unintentional manipulations (often referred to as "atacks"). Robustness [12] measures the ability of watermarking schemes of preserving the embedded marks, whereas security concerns are related to the use of secret keys which make the watermarking scheme more difficult to attack by a malicious opponent.

In order to endorse the watermarking system described above with robustness against attacks and also to introduce security measures, several modifications are introduced in [13][1]. The main features introduced in that paper are the following:

- The frequency band for mark embedding is chosen according to the difference between the original audio and an MP3-compressed version of the audio file. The frequency band is chosen such that the FFT magnitudes of the original and the compressed audio files is below some threshold.

- The scaling parameter s (was q in [11]) is chosen such that the number of embedding positions satisfies a minimum capacity requirement (as far as this minimum is feasible).

- An automatic procedure is presented to choose both the frequency band and the scaling parameter s.

- Once the tuning parameters (frequency band and s) are available, their valued are embedded at specific positions of the spectrum such that the detector can recover them. The position of these values are not fixed, but generated using a Pseudo-Random Number Generator (PRNG). In addition, the values are not embedded as clear text, but also scrambled as the XOR-sum between the true values and a Pseud-Random Binary Sequence (PRBS). The seeds of the PRNG and the PRBS are required as the secret key both at the embedder and the extractor.

- The method has been combined with the self-synchronising strategy presented in [14]. This strategy makes it possible to divide long audio files

[1] This paper has been accepted for publication in IEICE Transactions on Information and Systems.

into blocks of a give length (*e.g.* 10 seconds) and mark each of the blocks independently. Each block is preceded by a time-domain synchronisation watermark which can be detected in real-time.

- This method provides robustness against most of the attacks in the Stirmark Benchmark for Audio (SMBA) [15], capacity around 3 kbps (somewhat lower than that of the audio data hiding system of [11]) and excellent transparency (ODG around -0.5).

In the paper [16], we take a completely different approach. This work prioritises transparency and CPU time (efficiency), such that the suggested method can be used in real-time applications, such as broadcast monitoring systems. The method can be summarised as follows:

- Synchronisation marks are embedded in the time domain by disturbing a set of consecutive samples. For each set of samples, the internal values are compared with the straight line which connects the first and the last sample. If the internal values are above the line, then it is considered as a '1'. If the the internal values are below the line, a '0' is embedded. This embedding condition is very fast to be checked in real-time systems, and does not produce detectable distortions in the audio file. In addition, it overcomes some of the drawbacks found in other strategies (such as that of [14]), since the audible clicks which can be perceived with that technique are avoided.

- As the information watermark is concerned, the suggested method stems from the results of the schemes presented in [17, 18], 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 [17, 18]) 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 order 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 embedding method of the information watermark consists of sorting the FFT magnitudes in a given segment. Then a given condition is enforced for the values of 4 consecutive FFT magnitudes (once sorted).

- As security is concerned, the use of a secret key is required both for mark embedding and mark extraction. The secret parameters required in the scheme are the following: the synchronisation segment and its length, the number of samples used for embedding the synchronisation bits, the length of the information mark, the number of samples used to embed the bits of the information mark and the position of the ordered sequence of the FFT magnitudes to embed the information bits.

- In this case, since capacity is not a priority, low embedding capacity is achieved (around 16 bps) but transparency is very high (average ODG is -0.12) and robustness is achieved against typical signal processing attacks.

Finally, we have obtained another result for robust watermarking in the FFT domain [19]. In this paper, the chosen embedding and detecting approach is completely different, since it is based on interpolated values of the FFT magnitudes. The aim of the proposed method was to develop a high bit-rate audio watermarking technique with robustness against common attacks and good transparency.

- This algorithm is based on the difference between the original and the interpolated amplitudes of the FFT samples as obtained using the spline interpolation. The ratio between the interpolated error to the interpolated sample and the selected frequency band are the tuning parameters of this method. These parameters can be selected adaptively to regulate the capacity, the perceptual distortion and the robustness of the scheme.

- The experimental results show that this scheme has a high capacity (about 3 kbps) without significant perceptual distortion (ODG about -0.5) and provides robustness against common signal processing attacks such as echo, noise, filtering, resampling, and MPEG compression (MP3).

- Besides, the CPU time required by the scheme is short enough (about 20% of the playing time) to use it in real-time applications.

2.2 Methods in the DWT domain

Apart from the results achieved in the FFT domain, we have started a new research line of audio watermarking methods in the Discrete Wavelet Transform (DWT) domain. The idea of the new methods is to enhance the robustness of the watermarking systems for a greater range of the attacks which can be survived with the FFT techniques and, at the same time, preserve the capacity and transparency results of the FFT-based approaches introduced in the previous section. The main results achieved in the DWT domain have been submitted to two journals for publication.

The first result is presented in [20][2]:

- This method uses the last high frequency band of the third level wavelet decomposition (DDD) of the Daubechies 8 wavelet transform. This band is divided into small frames and the average of each frame is used as a reference value to change the value of the chosen samples. These reference values are the same in the coder/decoder or sender/receiver. In this algorithm, we divide each element by the average of the corresponding frame

[2]This paper has been accepted for publication in IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences.

and, then, all wavelet samples with value in the range $[-k, k]$ are used for embedding, where k is the embedding interval value. If the corresponding secret bit is '0', the sample in this interval is changed to $-m_i$ and, if it is '1', the corresponding sample is changed it to $+m_i$, where m_i is the mean of the i-th frame.

- The experimental results show that high capacity (5.5 kbps), remarkable transparency (ODG around -0.5) and robustness against most common attacks in the SMBA and MP3 compression are achieved. In fact, the results obtained with this method overcome those of the FFT-based systems detailed above.

However, the method presented in [20] requires the use of the whole audio file both for embedding and extracting. In addition, a deep analysis on how the system can be tuned or the influence of the different parameters on the key properties (robustness, capacity and transparency) is not provided. These drawbacks are overcome in the method described in [21], which stems from the results given in [20], but provides several improvements:

- The frequency band used for embedding is the last high frequency band of the second level wavelet decomposition (DD) of the Daubechies wavelet transform. This choice does not affect the transparency and robustness results in a significant way compared to the results of [20], but it doubles the capacity of the watermarking scheme.

- The scheme is also implemented in a block-based manner. The audio files are divided into blocks of a given length (10 seconds) and time-domain synchronisation marks are used to identify the beginning of each block. These synchronisation marks can be detected very efficiently in real-time applications.

- The scheme provides excellent perceptual quality of the marked contents (ODG about -0.7), robustness against the attacks in the SMBA and the highest capacity (11 kbps) among all the robust watermarking systems we have designed. In fact, no results of robust audio watermarking with such a high capacity have been found in the reviewed literature.

Chapter 3

Fingerprinting and steganography

Apart from the watermarking schemes presented in the previous chapter, we have obtained several results which can be applied in security applications for audio contents (and also for other types of multimedia information). This chapter presents some fingerprinting and steganography results.

3.1 Fingerprinting

In contrast to watermarking (which allows ownership protection), fingerprinting is a technique which allows to track redistributors of electronic information. In a fingerprinting scheme, each copy image is marked with a different mark that allows buyer identification. Usually, it is assumed that two or more dishonest buyers can only locate and delete marks by comparing their copies (marking assumption, [22]).

3.1.1 Fingerprinting codes

Fingerprinting codes are used to prevent dishonest users from redistributing copyrighted material. In this context, codes with the traceability (TA) property are of remarkable significance, since they provide an efficient way to identify traitors. Codes with the identifiable parent property (IPP) are also capable of identifying traitors, requiring less restrictive conditions than the TA codes at the expense of not having an efficient decoding algorithm, in the general case. Other codes that have been widely studied but possess a weaker traitor-tracing capability are the secure frameproof codes (SFP). It is a well-known result that TA implies IPP and IPP implies SFP. The converse is in general false. However, it has been conjectured that for Reed-Solomon codes all three properties are equivalent. We have investigated this equivalence and so far have provided positive answer:

1. For families of Reed-Solomon codes when the number of traitors divides the size of the code field [23]

2. For a $[n, k, d]$ Reed-Solomon codes, defined over a field that contains the $(n - d)$ roots of unity [24]

These results answer a question posted by Silverberg *et al.* in [25] for a large family of Reed-Solomon codes.

In this same way, we have worked in the use of convolutional codes as fingerprinting codes. In this sense, our contributions have been:

1. The improvement of collusion secure convolutional fingerprinting information codes in order to obtain a bound to quantify the false positive rate produced by this kind of codes. On the other side, some guidelines for a correct design of this family of codes was also given. By means of these guidelines, the false positive rate can be highly improved. This work is discussed in [26].

2. Taking into account that Turbo codes performance is higher than convolutional codes, the contribution entitled 'New considerations about the correct design of turbo fingerprinting codes' was presented in [27], in order to use turbo codes instead of convolutional codes. The major contribution of this paper is a new analysis of turbo fingerprinting codes that shows its potential drawbacks. Moreover, the identification of these drawbacks allows to discuss an entirely new construction of fingerprinting codes based on turbo codes.

One of the most important problem of fingerprinting codes is their suitability in order to be included in a real application in which they work together with watermarking systems. In this sense, we have worked in the adaptation of informed coding and informed embedding (two watermarking techniques), in order to adapt them for its use in fingerprinting schemes. This work was published in [28].

Moreover, in [29] we have analysed the performance of using together fingerprinting codes and watermarking techniques over video contents and the effect produced over this mark by a collusion attack and the upload to YouTube service. We shown that tracing traitors is possible over YouTube service if the watermarking algorithm is carefully configured and the fingerprinting are correctly chosen.

Another topic in we have devoted lots of effort has been the use of watermarking algorithms in order to protect the correct execution of mobile agents. As a result of this efforts two contributions have been published:

1. In [30] we propose a new technique based on the embedding of a matrix of marks in each transceiver of the IDS in order to guarantee that the agents are properly executed.

2. In [31] we have proposed an improvement of the Self-Validating Branch-Based Software Watermarking by Myles *et al.* in order to guarantee that the software is being executed correctly by a non trusted host. The proposed modification is the incorporation of an external element called sentinel which controls branch targets.

3.1.2 Asymmetric fingerprinting

Classical fingerprinting schemes [32, 22] are symmetrical in the sense that both the seller and the buyer know the fingerprinted copy. Even if the seller succeeds in identifying a dishonest buyer, her previous knowledge of the fingerprinted copies prevents her from using them as a proof of redistribution in front of third parties. In [33], the concept of asymmetric fingerprinting was introduced, whereby only the buyer knows the fingerprinted copy. Different asymmetric fingerprinting proposals can be found in the literature [33, 34, 35, 36, 37, 38, 39].

Watermarking in the encrypted domain can offer new possibilities towards the construction of new asymmetric fingerprinting schemes. In [40], we have presented a theoretical approach on the properties that a watermarking scheme and a cryptosystem should provide in order to design an asymmetric fingerprinting scheme.

As already mentioned, a watermarking scheme can be defined with two functions, the embedding or marking function $\mathcal{M}$ and the extraction or verification function $\mathcal{V}$. Roughly speaking, the marking function takes the cover object I (an audio file or some other multimedia content) as an input together with the mark m to be embedded and produces the marked object $I^* = \mathcal{M}(I, m)$. On the other side, the verification function takes the marked (and possibly distorted) object $\widehat{I}$ and gives the mark embedded in the object $\mathcal{V}(\widehat{I}) = m$.

We denote the encryption function $\mathcal{E}$ with a encrypting key k that produce a encrypted object $I_k = \mathcal{E}_k(I)$. The decryption function $\mathcal{D}$ produces the clear object $I = \mathcal{D}_{k^{-1}}(I_k)$ given the decrypting key k^{-1} and the encrypted object I_k.

Depending on where each function is applied different properties can be satisfied:

Prop. 1 The marking function $\mathcal{M}$ can be executed in an encrypted object I_k to embed a mark m.

Prop. 2 The verification function $\mathcal{V}$ can be able to reconstruct a mark in the encrypted domain when it has been embedded in the encrypted domain.

Prop. 3 The verification function $\mathcal{V}$ can be able to reconstruct a mark in the encrypted domain when it has been embedded in the clear domain.

Prop. 4 The decryption function does not affect the mark integrity in terms of mark reconstruction process.

Property 1 ensures that when the marking function is performed over an encrypted object, the result $I_k^* = \mathcal{M}(I_k, m)$ will have some sense. This point

is relevant since the marking schemes in the literature are based on object characteristics that may disappear when the object is encrypted.

The second property ensures that the mark and verification process can be performed entirely in the encrypted domain

$$\mathcal{V}(\mathcal{M}(\mathcal{E}_k(I), m)) = m.$$

The third property means that the encryption function does not affect the mark integrity in terms of mark reconstruction process and it holds if

$$\mathcal{D}_{k^{-1}}(\mathcal{V}(\mathcal{E}_k(\mathcal{M}(I, m)))) = m.$$

Notice that properties 2 and 3 are equivalent in case the marking function and the encryption function commute

$$\mathcal{M}(\mathcal{E}_k(I), m) = \mathcal{E}_k(\mathcal{M}(I, m)) = I_k^*.$$

The last property implies that

$$\mathcal{V}(\mathcal{D}(\mathcal{M}(\mathcal{E}_k(I), m))) = m.$$

At first glance, it could be difficult to determine encryption/decryption functions and watermarking algorithms that hold all the proposed properties. For instance, as it has been pointed out, Property 1 fails for the vast majority of marking schemes in the literature since to achieve imperceptibility they are based on object characteristics that disappear when the object is encrypted.

However, in some scenarios, an interesting secure protocol can be defined only with one of the proposed properties. A clear example is the verification protocol proposed in [41] that allows to demonstrate the presence of a watermarking in an object without revealing the mark, thus producing the first approach to a zero-knowledge watermarking verification protocol. In this case, the watermarking verification protocol proposed is based on any linear and additive watermarking algorithm in which the watermarking verification can be performed by mark correlation (for instance the spread spectrum technique proposed by Cox *et al.* [42]). The encryption algorithm used is the RSA. When using such watermarking techniques together with this encryption algorithm Property 3 holds due to the homomorphic properties of the RSA algorithm together with the multiplicative operations performed in the verification process. This example shows the possibilities of watermarking in the encrypted domain, even if only one of the properties holds.

If we assume functions $\mathcal{M}$, $\mathcal{V}$, $\mathcal{E}$, $\mathcal{D}$ hold the properties stated above we can define new protocols with some interesting properties as it is shown in the next subsection.

As an example of a possible application, consider the following scenario.

Suppose functions $\mathcal{M}$, $\mathcal{V}$, $\mathcal{E}$, $\mathcal{D}$ hold the four properties stated above. Suppose the watermarking scheme used is asymmetric in the sense that a different secret information is needed for embedding and verifying the mark [43]. Finally, suppose the function $\mathcal{E}$ is a commutative encryption function.

With these assumptions, we have defined [40] a theoretical asymmetric fingerprinting scheme based on a protocol between the seller, S, and the buyer, B that allows to embed a mark into an object in a way that: *a)* only B obtains the marked image, an *b)* only S knows the original image.

3.2 Steganographic codes

Steganography is a specific information hiding application which aims to hide secret data imperceptibly into a commonly used media, such as a digital image or an audio file.

An early and easy way to hide information in JPG images is by using Least Significant Bit (LSB) steganography. This method is applied in the image frequency domain, that is, after performing a discrete cosine or a wavelet transformation in the spatial image. Then, we represent the image as a sequence of integer-valued symbols, where each symbol is represented by B binary digits. LSB only considers the least significant bit in each symbol, and modifies these bits to hide information in the JPG file. This technique can be viewed as hiding two bits per changed bit in the cover message because, in a random case, 50% bits do not need to be changed. Thus, the basic LSB mechanism has a distortion rate of 0.5.

Some more interesting methods are based on binary linear codes. With the same distortion rate as LSB, they allow a greater embedding rate of secret information. In particular, most of the codes used in steganography are linear. The existence of a parity check matrix helps to design good protocols.

Let n and t be positive integers, $t \leq n$, and let X be a finite set. An embedding/retrieval steganographic protocol of type $[n, t]$ over X is a pair of maps $e : X^t \times X^n \longrightarrow X^n$ and $r : X^n \longrightarrow X^t$ such that $r(e(s, v)) = s$ for all $s \in X^t$ and $v \in X^n$. Maps e and r are the embedding and the retrieval maps, respectively. The number $\rho = max\{d(v, e(s, v))|\, s \in X^t, v \in X^n\}$, d being the Hamming distance, is the radius of the protocol.

The embedding map of a $[n, t]$ embedding/retrieval steganographic protocol with radius ρ (for short, a $[n, t, \rho]$ protocol) allows us to hide t information symbols into a string of n cover symbols, by changing a maximum of ρ of these cover symbols.

As discussed, there are two parameters which help to evaluate the performance of a steganographic protocol $[n, t, \rho]$: the average distortion $D = \dfrac{R_a}{n}$, where R_a is the expected number of changes over uniformly distributed messages, and the embedding rate $\dfrac{t}{n}$. In general, for the same embedding rate a protocol is better when the average distortion is smaller.

The theoretical hiding asymptotical capacity of steganographic systems is not attained by algorithms developed so far. Our work consists in the design of an efficient steganographic protocol with the aim to improve the capacity of today's steganographic systems [44]. The proposed technique does not use

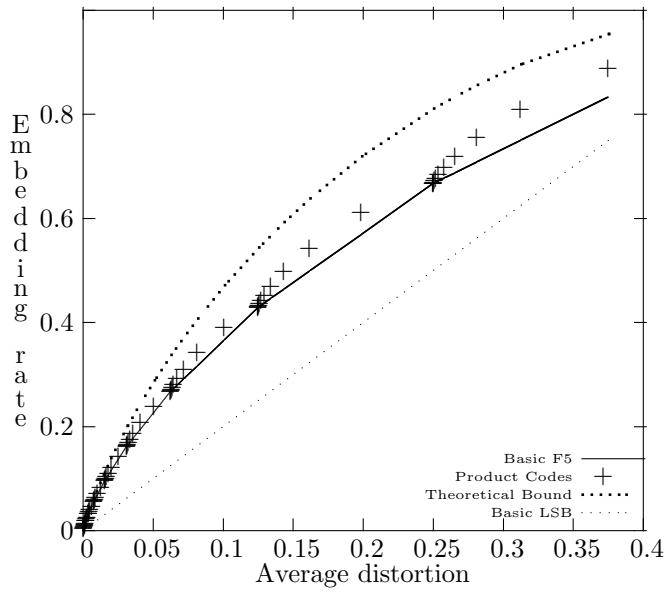

Figure 3.1: Performance of steganographic codes. The embedding rate as a function of the average distortion.

linear codes in the same way that traditional code-based protocols (F5), but uses a product code of two Hamming codes.

Let C_1 and C_2 be two Hamming codes of length $n_1 = 2^x - 1$ and $n_2 = 2^y - 1$, respectively. The product code $C_1 \otimes C_2$ is the code of length $n = (2^x - 1)(2^y - 1)$, dimension $k = (n_1 - x)(n_2 - y)$ and with the peculiarity that their codewords can be seen as $(2^y - 1) \times (2^x - 1)$ matrices, where the rows are codewords in C_1 and the columns are codewords in C_2. The constituent perfect codes of the product code are used in such a way that it it is possible to embed and retrieve hidden bits in a cover source obtaining smaller average distortion R_a/n than that obtained using only perfect codes with the same embedding rate t/n.

In figure 3.1, the performance of the designed code for different values of the parameters is depicted. The obtained results show that, with the same average distortion rate, the embedding rate of the designed code is greater than that of the LSB basic steganography of F5 algorithm.

On the other hand, the designed protocol is highly efficient. It is based on Hamming codes and both, the embedding and the retrieval algorithm, have the same computational cost as in the F5 case.

Chapter 4

Contributions in the image field

The groups which carry out research in the watermarking field do not usually focus on a single type of multimedia contents. For this reason, we have obtained several results also in the image field. These results are briefly summarised in this chapter.

4.1 Semi-fragile watermarking of hyperspectral images

We have designed a semi-fragile watermarking method [45][1] for multi and hyperspectral images based on Tree Structured Vector Quantisation (TSVQ) and compression. The method uses the information in all the bands at the same time, and thus, it takes advantage of both spatial and spectral redundancy for marking purposes. Basically, the original image is segmented in three dimensional blocks and a tree structured vector quantiser is built for each block together with a Least Significant Bits (LSB) extracting process. The original block is replaced by a new one generated by substituting each original vector by the closest centroid in the selected subtree. This process is repeated until a certain stopping criterion is satisfied. Each block generates a different subtree and a secret key is used to avoid copy-and-replace attacks between blocks.

The results show that copy-and-replace attack of a region of the image is detected by the watermarking scheme, whereas near-lossless (JPEG2000 or JPEG) compression can be applied up to some ratio preserving the mark in the compressed image. The detection process is a simple one, since a tree is built for each block and the selected tree property is tested. If a block satisfies such a

[1] This paper has been submitted to an ISI-indexed journal. The reviewers are currently evaluating the second version of the manuscript with the changes introduced in the paper according to their comments.

property, then it has not been forged, otherwise the detection process report tampering.

The following steps summarise the mark embedding process:

0. Pre-processing: compression and decompression of the original image with JPEG2000 (KaKaDu Software) [46].
1. Band selection and block construction of the image to be marked.
2. Extract n Least Significant Bits (LSB) for each pixel component.
3. Choose the seed of a Pseudo-Random Number Generator (PRNG) and initialise it.
4. Choose the mark property (*e.g.* entropy).
5. For all blocks
   - 5.1 Generate a number with the PRNG and check it is not repeated for a previous block.
   - 5.2 Choose the property (entropy) according to the number generated in step 5.1.
   - 5.3 Select the Tree Structured Vector Quantisation (TSVQ) tree with the entropy value chosen in step 5.2.
   - 5.4 Generate the image using the tree obtained in step 5.3.
   - 5.5 Check the property selected in 5.2. If not checked go to 5.3 with the image generated in 5.4.
   - 5.6 Restore the LSB extracted in 2 minimising the difference of the pixel values.
6. Join all the blocks (and the bands not selected in step 1) to build the final marked image.

The mark detection process for a (possibly forged) image is analogous to the mark embedding process, and it only requires the seed of the pseudo-random sequence. First of all, the same bands used for embedding must be extracted from the marked image. Then, it must be divided into the same blocks to determine if the mark is present or if they have been modified (above a given threshold). The LSB must be extracted from the (assumed) marked block. For each block and the corresponding property for that block (computed from the PRNG), the detection process is performed.

The detection of a modification of the image can be performed by checking if the same criterion used in the mark embedding scheme is satisfied. Thus, the TSVQ tree is constructed for each block and the criterion is checked. If the block verifies the criterion then the area is assumed to be authenticated. Otherwise, the block is detected as forged. Therefore, with this method, it is possible to inspect and locate tampered regions in a marked image.

4.2 Image data hiding

Image data hiding is focused on embedding as much as information as possible into an image. In this case capacity is the priority, whereas robustness is not a desired objective of the schemes.

4.2.1 Data hiding for medical images

In applications where additional information is required to describe another information media, such process can be very useful. For instance, in medical images [47, 48], the patients' details and the doctors' views can be embedded into the medical images to form a comprehensive data bank. The integrity of such a concentrated database not only makes medical files very secure, but also their remote access by fellow doctors is possible. However, data hiding in medical images, due to their specific requirements, impose certain constraints which set some specific requirements. Firstly, medical images are required to be of high quality and hence the embedded data should be invisible. Secondly, data insertion may be gradually introduced. Indeed, during the creation of a medical file, it is undeniable to question the patient on his/her personal, family, social life and family conditions. As the patients get more acquainted with their doctors, or queries arise, the new information comes to be added to constitute a medical history of the patient. Moreover, the fellow doctors may also add their own observations. This necessitates frequent addition/insertion of medical information to the main file. Thus, not only the data hiding system has to be reversible, but 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. Consequently, high quality (fidelity), authentication, high capacity, frequent insertions and reversibility are the main requirements of medical files.

The histogram-shifted-based lossless data hiding algorithm proposed by Ni *et al.* [49] is one of the most capacity efficient data hiding system which suits medical images well. Recently, Lin *et al.* [50] suggested a high capacity and low distortion algorithm based on the differences between neighbouring pixels. In the paper [47], we introduce a highly efficient reversible data hiding technique. This technique is based on dividing the image into tiles and shifting the histograms of each image tile between its minimum and maximum frequencies. Data are then embedded into the pixel level with the largest frequency to maximise data hiding capacity. It exploits the special properties of medical images, where the histogram of their non-overlapping image tiles mostly peak around some gray values and the rest of the spectrum is mainly empty. The zeros (or minima) and peaks (maxima) of the histograms of the image tiles are then relocated to embed the data. The grey values of some pixels are therefore modified.

We show how histograms of image tiles of medical images can be exploited to achieve these requirements. Compared with the data hiding method applied to the whole image, our scheme can result in 30%-200% capacity improvement

with still better image quality, depending on the medical image content.

The main idea in the shifted-histogram data hiding method is to find a pair of maximum and minimum in the image pixel intensity histogram and then shift the intensity of those pixels within the maximum and minimum frequency range by one level, towards the minimum frequency level. This creates an empty space on the shifted histogram at the vicinity of the maximum pixel density. To embed a data stream, the modified image is re-scanned and when the pixel of maximum frequency is encountered if the corresponding bit in the embedding stream is "1" its gray level is incremented by one level, otherwise it is unaltered. Thus, the maximum number of bits that can be hidden into the image is equal to the maximum frequency of the original histogram. Due to the created gap, the data hiding mechanism is reversible. The values of the pixels with maximum and minimum frequencies are also recorded as side information. If the minimum frequency is non-zero, then their numbers also need to be embedded as side information, which reduces the data hiding capacity of the system.

In [48], we take advantage of the Region of non-Interest (RONI) and the Region of Interest (ROI), objective and subjective quality and analyse the properties of this scheme compared with Ni *et al.* [49]. Although Ni *et al.* [49] show that their algorithm for a vast variety of images outperforms almost all the known reversible data hiding methods so far, we believe that it has two relevant drawbacks for medical images:

1. If the intensity of the pixels in a region of interest lay in the maximum and minimum range of the histogram, then their values are also modified.

2. If the minimum frequency of the histogram is non-zero, the positions of all the pixels with minimum frequency have to be embedded as side information. This restricts the data hiding capacity of the system.

Now, if the image is partitioned into sub-images (the so-called image tiles) and the histogram shifting is applied to each image tile, not only the above shortfalls are overcome, but some additional benefits can be gained. These include:

1. Region of non-Interest (RONI): the image can be divided into parts such that only the histograms of the region of non-interest image tiles are modified and the data is hidden.

2. High payload: in the shifted-histogram based data hiding method, the maximum number of hidden bits (watermark signature) is equal to the maximum frequency of the pixel intensity histogram. When the histograms of the image tiles are considered separately, it is intuitive that the sum of individual maxima is greater than the maximum of the original image intensity histogram. Hence shifted-histograms of the image tiles can hide more watermark data.

3. Higher objective quality: In the shifted-histogram method, the quality of the marked image depends on the number of pixels whose intensity lay

between the maximum and minimum frequency pixel values, irrespective of the number of hidden bits. That is, image quality due to embedding one bit of data is as bad/good as if the maximum payload (equivalent to the maximum frequency of the intensity histogram) is embedded. On the other hand, with the histograms of image tiles, they may be first prioritised according to the order of their least intensity distance between the maximum and minimum frequencies. Data are embedded in the ordered image tiles till it is fully loaded and the leftover data will be embedded into the next image tile, and so on. In this manner, for a given payload, the intensity of the smallest number of pixels is modified and, hence, image quality will be at its best.

4. Higher subjective quality: rather than prioritising the image tiles as described above, they may be prioritised based on their spatial content. Data hiding can then start from those image tiles which have the highest spatial details. In this case, due to spatial masking of the human visual system, the subjective quality of the watermarked image will be at its best.

5. Narrower histogram: some image tiles have much narrower histograms than that of the whole image. This is particularly true for medical images, which leads to the following useful properties for data hiding:

   - In the broader histogram of the whole image, the minimum frequency may not be zero. Hence, for reversible data hiding, their positions need to be identified and given as side information, which greatly reduces the data hiding capacity. On the other hand, in the narrower histograms of the image tiles, the minimum frequencies are more likely to be zero.
   - Narrower histograms provide the opportunities of selecting the most suitable pairs of peaks-zeros which will increase the quality of the marked images.

In [48], we show how, by applying shifted-histogram procedur 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 on the region of non-interest and tradeoff between capacity and quality are also presented.

4.2.2 High capacity image data hiding

In [51], we propose a novel high capacity reversible image data hiding scheme using a prediction technique which is effective for error resilience in H.264/AVC. In the proposed method, which is based on H.264/AVC intra prediction, firstly, the prediction error blocks are computed and then the error values are slightly modified through shifting the prediction errors. The modified errors are used for embedding the secret data. The experimental results show that the proposed method, called shifted intra prediction error (SIPE), is able of hiding more secret

data compared to other schemes in the literature, while the PSNR of the marked image is about 48 dB.

The SIPE scheme is based on increasing the differences between pixels of the cover image and their intra prediction values. The prediction error at which the number of prediction errors is at a maximum is selected to embed the message. The prediction errors larger than the selected error are increased by "1". Furthermore, the selected prediction error is left unchanged and increased by "1" if the embedded bit is "0" and "1", respectively. The SIPE method is able to embed a huge amount of data (15-120 kbits for a $512 \times 512 \times 8$ greyscale image) while the PSNR of the marked image versus the original image is about 48 dB. In addition, simplicity and applicability to almost all types of images and H.264 video coding make this method superior to most of existing reversible data hiding techniques. Although the proposed lossless data hiding technique is applied to still images, it is very useful for H.264/AVC because the insertion of additional information only needs the shifting and embedding steps in the coding steps. Furthermore, this lossless technique will not degrade the video quality.

In [52], we propose the adaptive shifted prediction error (ASPE) method. This method is based on hiding data at the locations of larger differences between the pixels of the cover image and their prediction values to exploit the spatial masking of the human visual system. In this way, as long as the interfering hidden data is under the perceptual threshold, the embedded information will not be perceptible. Since larger prediction errors, which normally occur at edges or in highly textured areas, have higher spatial masking, they are ideal for hiding the data. To gain larger masking effect with maximum data hiding capacity, the prediction error at which the number of prediction errors is equal or larger than the needed capacity is selected to embed the message. Thus, one can trade visual quality for the embedding capacity. The ASPE method is able to embed a huge amount of data (15-120 kbits for a $512 \times 512 \times 8$ grayscale image) while guaranteeing the PSNR of the marked image with respect to the original image to be above the perceptual threshold of human visual system (*e.g.* 40 dB). Moreover, for a given capacity the data are hidden at the maximum possible prediction error, making the subjective quality even more impressive due to the special masking. In addition, simplicity, short execution time and applicability to almost all types of images make this method superior to most of the existing reversible data hiding techniques.

Chapter 5

Conclusions and list of contributions

5.1 Conclusions

The results presented in this Deliverable Report are included in WP3: Secure Electronic Commerce and Digital Content Distribution of the ARES Project and, more precisely, cover the following objectives of this Work Package:

- *The objective of the DRM systems is to allow the content owners to control the digital content and obtain as a result the protection of electronic copyright. In fact, the main components of a DRM system are encryption, access control, copy control, identification and tracing.*
- *In order to improve the properties of the DRM systems, the ARES team intend to deal mainly with marking techniques because these can be applied to both copy control and identification, as well as to traceability of contents. The objectives of ARES related to digital rights management are the following: improve the reliability of the watermarking scheme; design semi-fragile watermarking schemes (useful to check the integrity of the content), implement asymmetric watermarking systems (such that the content seller does not see the marked contents if the buyer is honest), implement asymmetric fingerprinting schemes and improve the evaluation techniques of marking schemes.*

The audio watermarking schemes presented in Chapter 2 are completely aligned with these objectives. All the presented schemes are blind, robust and most of them incorporate security issues (through the use of secret keys). In addition, high capacity, excellent transparency and short CPU-time are the common properties of all the developed schemes, which makes them particularly useful in different applications, such as proof of ownership, copy detection and broadcast monitoring.

The fingerprinting and steganography schemes described in Chapter 3 go one step forward in the copy detection field, since they make it possible to identify traitorous buyers who try to remove the copyright protection information which is embedded into the media files using some robust and secure watermarking scheme. These schemes will make it possible to develop secure e-commerce tools for multimedia contents which guarantee the protection of the contents,the copyright owners and also the buyers (who are protected against potentially malicious sellers).

Finally, the methods presented in Chapter 4 provide with tools which make it possible to check the integrity and the authenticity of sensitive information (such as medical and remote sensing images). Some of the methods described in that chapter do not only report the authenticity of the content, but also the tamper locations if the image has been forged.

5.2 List of contributions

The following papers have been published or submitted by members of the ARES groups.

5.2.1 Audio watermarking

1. M. Fallahpour and D. Megías, "High Capacity Method for Real-Time Audio Data Hiding Using the FFT Transform," in *Communications in Computer and Information Science*, J. H. Park, J. Zhan, C. Lee, G. Wang, T.-H. Kim, and S.-S. Yeo, Eds., vol. 36. Springer Berlin Heidelberg, 2009, pp. 91–97.

2. M. Fallahpour and D. Megías, "Robust high-capacity audio watermarking based on FFT amplitude modification," *IEICE Trans. on Information and Systems*, 2009, accepted for publication.

3. D. Megías, J. Serra-Ruiz, and M. Fallahpour, "Efficient self-synchronised blind audio watermarking system based on time domain and FFT amplitude modification," submitted.

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

5. M. Fallahpour and D. Megías, "DWT-based high capacity audio watermarking," *IEICE Trans. on Fundamentals of Electronics, Communications and Computer Sciences*, 2009, accepted for publication.

6. M. Fallahpour and D. Megías, "High capacity audio watermarking using the high frequency band of the wavelet domain," submitted.

5.2.2 Fingerprinting and steganography

7. J. Moreira, M. Fernandez, and M. Soriano, "A note on the equivalence of the traceability properties of Reed-Solomon codes for certain coalition sizes," *IEEE Workshop on Information Forensics and Security*, 2009, in press.

8. M. Fernandez, J. Cotrina, and N. D. M. Soriano, "On the ipp properties of Reed-Solomon codes," *IFIP SEC09*, 2009, in press.

9. J. Tomàs-Buliart, M. Fernandez, and M. Soriano, "Improvement of collusion secure convolutional fingerprinting information codes," *Information Theoretic Security Second International Conference, ICITS 2007*, vol. Lecture Notes in Computer Science 4883, pp. 76–87, 2007.

10. J. Tomàs-Buliart, M. Fernandez, and M. Soriano, "New considerations about the correct design of turbo fingerprinting codes," in *ESORICS*, 2008, pp. 501–516.

11. J. Tomàs-Buliart, M. Fernandez, and M. Soriano,"Using informed coding and informed embedding to design robust fingerprinting embedding systems," in *KES (3)*, 2007, pp. 992–999.

12. J. Tomàs-Buliart, M. Fernandez, and M. Soriano, "Traitor tracing over youtube video service - proof of concept," *Accpted at Journal on Telecommunication Systems*, 2008.

13. R. Páez, J. Tomàs-Buliart, J. Forné, and M. Soriano, "Securing agents against malicious host in an intrusion detection system," *2nd International Workshop on Critical Information Infrastructures Security (CRITIS 2007)*, vol. Lecture Notes in Computer Science 5141, 2007.

14. J. Tomàs-Buliart and M. M.Fernández, "Protection of mobile agents execution using a modified self-validating branch-based software watermarking with external sentinel," *Critical Information Infrastructure Security Third International Workshop, CRITIS 2008*, vol. Lecture Notes in Computer Science 5508, pp. 287–294, 2008.

15. J. Herrera-Joancomartí and D. Megías, "Watermarking in the encrypted domain," in *Congreso Iberoamericano de Seguridad Informática*, Montevideo, Uruguay, 2009, in press.

16. H. Rifà-Pous and J. Rifà, "Product perfect codes and steganography," *Digit. Signal Process.*, vol. 19, no. 4, pp. 764–769, 2009.

5.2.3 Image watermarking

17. J. Serra-Ruiz and D. Megías, "A novel semi-fragile forensic watermarking scheme for remote sensing images," submitted.

18. M. Fallahpour, D. Megías, and M. Ghanbari, "High capacity, reversible data hiding in medical images," in *IEEE International Conference on Image Processing (ICIP2009)*. Los Alamitos, CA, USA: IEEE Computer Society, 2009, in press.

19. M. Fallahpour, D. Megías, and M. Ghanbari, "High capacity and reversible data hiding in medical images," submitted.

20. M. Fallahpour and D. Megías, "Reversible data hiding based on h.264/avc intra prediction," in *IWDW*, ser. Lecture Notes in Computer Science, Y. Q. Shi, H.-J. Kim, and S. Katzenbeisser, Eds., vol. 5041. Springer-Verlag, 2009, in press.

21. M. Fallahpour, D. Megías, and M. Ghanbari, "Subjectively adapted high capacity lossless image data hiding based on prediction errors," submitted.

Bibliography

[1] H. H. Yu, D. Kundur, and C.-Y. Lin, "Spies, thieves, and lies: The battle for multimedia in the digital era," *IEEE MultiMedia*, vol. 8, no. 3, pp. 8–12, 2001.

[2] I. Cox, M. Miller, and J. Bloom, *Digital Watermarking*. San Francisco, CA, USA: Morgan Kaufmann, 2003.

[3] M. Wu and B. Liu, *Multimedia Data Hiding*. New York, CA, USA: Springer-Verlag, 2003.

[4] D. Kundur, "Watermarking with diversity: Insights and implications," *IEEE MultiMedia*, vol. 8, no. 4, pp. 46–52, 2001.

[5] J. A. Bloom, I. J. Cox, T. Kalker, J. paul Linnartz, M. L. Miller, and C. B. Traw, "Copy Protection for DVD Video," in *Proceedings of the IEEE*, 1999, pp. 1267–1276.

[6] J. J. Eggers and B. Girod, *Informed Watermarking*. Boston, MA, USA: Kluwer, 2002.

[7] W. Bender, D. Gruhl, and N. Morimoto, "Techniques for data hiding," in *Proceedings of SPIE*, vol. 2420. SPIE, 1995, pp. 40–48.

[8] I. J. Cox and M. L. Miller, "The first 50 years of electronic watermarking," *EURASIP J. Appl. Signal Process.*, vol. 2002, no. 2, pp. 126–132, 2002.

[9] F. Hartung and M. Kutter, "Multimedia watermarking techniques," *EURASIP J. Appl. Signal Process.*, vol. 87, pp. 1079–1107, 1992.

[10] M. D. Swanson, B. Zhu, and A. H. Tewfik, "Current state olf the art, challenges and future directions for audio watermarking," *Multimedia Computing and Systems, International Conference on*, vol. 1, p. 9019, 1999.

[11] M. Fallahpour and D. Megías, "High Capacity Method for Real-Time Audio Data Hiding Using the FFT Transform," in *Communications in Computer and Information Science*, J. H. Park, J. Zhan, C. Lee, G. Wang, T.-H. Kim, and S.-S. Yeo, Eds., vol. 36. Springer Berlin Heidelberg, 2009, pp. 91–97.

[12] J. Dittmann, D. Megías, A. Lang, and J. Herrera-Joancomartí, "Theoretical framework for a practical evaluation and comparison of audio watermarking schemes in the triangle of robustness, transparency and capacity," *Transactions on Data Hiding and Multimedia Security*, vol. Lecture Notes in Computer Science 4300, pp. 1–40, October 2006.

[13] M. Fallahpour and D. Megías, "Robust high-capacity audio watermarking based on FFT amplitude modification," *IEICE Trans. on Information and Systems*, 2009, accepted for publication.

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

[15] A. Lang, "StirMark Benchmark for Audio," http://amsl-smb.cs.uni-magdeburg.de. Last checked on September 30th, 2009.

[16] D. Megías, J. Serra-Ruiz, and M. Fallahpour, "Efficient self-synchronised blind audio watermarking system based on time domain and FFT amplitude modification," submitted.

[17] 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 - CMS 2003*, ser. Lecture Notes in Computer Science 2828. Turin (Italy): Springer-Verlag, October 2003, pp. 226–238.

[18] ——, "Total disclosure of the embedding and detection algorithms for a secure digital watermarking scheme for audio," in *ICICS'05: Proceedings of the Seventh International Conference on Information and Communication Security*, Beijing, China, December 2005.

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

[20] ——, "DWT-based high capacity audio watermarking," *IEICE Trans. on Fundamentals of Electronics, Communications and Computer Sciences*, 2009, accepted for publication.

[21] ——, "High capacity audio watermarking using the high frequency band of the wavelet domain," submitted.

[22] D. Boneh and J. Shaw, "Collusion-secure fingerprinting for digital data," in *Advances in Cryptology-CRYPTO'95*, ser. LNCS 963. Springer-Verlag, 1995, pp. 452–465.

[23] J. Moreira, M. Fernandez, and M. Soriano, "A note on the equivalence of the traceability properties of Reed-Solomon codes for certain coalition sizes," *IEEE Workshop on Information Forensics and Security*, 2009, in press.

[24] M. Fernandez, J. Cotrina, and N. D. M. Soriano, "On the ipp properties of Reed-Solomon codes," *IFIP SEC09*, 2009, in press.

[25] A. Silverberg, J. Staddon, and J. L. Walker, "Applications of list decoding to tracing traitors." *IEEE Transactions on Information Theory*, vol. 49, no. 5, pp. 1312–1318, 2003.

[26] J. Tomàs-Buliart, M. Fernandez, and M. Soriano, "Improvement of collusion secure convolutional fingerprinting information codes," *Information Theoretic Security Second International Conference, ICITS 2007*, vol. Lecture Notes in Computer Science 4883, pp. 76–87, 2007.

[27] J. Tomàs-Buliart, M. Fernandez, and M. Soriano, "New considerations about the correct design of turbo fingerprinting codes," in *ESORICS*, 2008, pp. 501–516.

[28] ——, "Using informed coding and informed embedding to design robust fingerprinting embedding systems," in *KES (3)*, 2007, pp. 992–999.

[29] J. Tomàs-Buliart, M. Fernandez, and M. Soriano, "Traitor tracing over youtube video service - proof of concept," *Accpted at Journal on Telecommunication Systems*, 2008.

[30] R. Páez, J. Tomàs-Buliart, J. Forné, and M. Soriano, "Securing agents against malicious host in an intrusion detection system," *2nd International Workshop on Critical Information Infrastructures Security (CRITIS 2007)*, vol. Lecture Notes in Computer Science 5141, 2007.

[31] J. Tomàs-Buliart and M. M.Fernández, "Protection of mobile agents execution using a modified self-validating branch-based software watermarking with external sentinel," *Critical Information Infrastructure Security Third International Workshop, CRITIS 2008*, vol. Lecture Notes in Computer Science 5508, pp. 287–294, 2008.

[32] G. R. Blakley, C. Meadows, and G. B. Purdy, "Fingerprinting long forgiving messages," in *Advances in Cryptology-CRYPTO'85*, ser. LNCS 218. Springer-Verlag, 1986, pp. 180–189.

[33] B. Pfitzmann and M. Schunter, "Asymmetric fingerprinting," in *Advances in Cryptology-EUROCRYPT'96*, ser. LNCS 1070. Springer-Verlag, 1996, pp. 85–95.

[34] B. Pfitzmann and M. Waidner, "Asymmetric fingerprinting for larger collusions," in *Proceedings of the 4th ACM Conference on Computer and Communicatios Security*, 1997, pp. 151–160.

[35] J. Domingo-Ferrer, "Anonymous fingerprinting of electronic information with automatic identification of redistributors," *Electronics Letters*, vol. 34, no. 13, pp. 1303–1304, June 1998.

[36] ——, "Anonymous fingerprinting based on committed oblivious transfer," in *Public key cryptography, PKC'99*, ser. LNCS 1560, H. Imai and Y. Zheng, Eds. Springer-Verlag, 1999, pp. 43–52.

[37] B. Pfitzmann and A. Sadeghi, "Coin-based anonymous fingerprinting," in *Advances in Cryptology - EUROCRYPT'99*. Berlin: Springer-Verlag, 1999, pp. 150–164, lecture Notes in Computer Science Volume 1592.

[38] A.-R. Sadeghi, "How to break a semi-anonymous fingerprinting scheme," in *Information Hiding - IH'01*, I. Moskowitz, Ed. Berlin: Springer-Verlag, 2001, pp. 384–394, lecture Notes in Computer Science Volume 2137.

[39] J.-G. Choi, J.-H. Park, and K.-R. Kwon, "Analysis of cot-based fingerprinting schemes: New approach to design practical and secure fingerprinting scheme," in *Information Hiding - IH'04*, J.Fridrich, Ed. Berlin: Springer-Verlag, 2004, pp. 253–265, lecture Notes in Computer Science Volume 3200.

[40] J. Herrera-Joancomartí and D. Megías, "Watermarking in the encrypted domain," in *Congreso Iberoamericano de Seguridad Informática*, Montevideo, Uruguay, 2009, in press.

[41] K. Gopalakrishnan, N. Memon, and P. L. Vora, "Protocols for watermark verification," *IEEE MultiMedia*, vol. 8, no. 4, pp. 66–70, 2001.

[42] I. J. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Transactions on Image Processing*, vol. 6, no. 12, pp. 1673–1687, 1997.

[43] T. Furon and P. Duhamel, "An asymmetric public detection watermarking technique," in *IH '99: Proceedings of the Third International Workshop on Information Hiding*. Springer-Verlag, 2000, pp. 88–100.

[44] H. Rifà-Pous and J. Rifà, "Product perfect codes and steganography," *Digit. Signal Process.*, vol. 19, no. 4, pp. 764–769, 2009.

[45] J. Serra-Ruiz and D. Megías, "A novel semi-fragile forensic watermarking scheme for remote sensing images," submitted.

[46] D. Taubman, "Kakadu JPEG-2000 encoder v4.2," 2001, `http://www.kakadusoftware.com`.

[47] M. Fallahpour, D. Megías, and M. Ghanbari, "High capacity, reversible data hiding in medical images," in *IEEE International Conference on Image Processing (ICIP2009)*. Los Alamitos, CA, USA: IEEE Computer Society, 2009, in press.

[48] ——, "High capacity and reversible data hiding in medical images," submitted.

[49] 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.

[50] C.-C. Lin, W.-L. Tai, and C.-C. Chang, "Multilevel reversible data hiding based on histogram modification of difference images," *Proc. IEEE*, vol. 41, no. 12, pp. 3582–3591, 2008.

[51] M. Fallahpour and D. Megías, "Reversible data hiding based on h.264/avc intra prediction," in *IWDW*, ser. Lecture Notes in Computer Science, Y. Q. Shi, H.-J. Kim, and S. Katzenbeisser, Eds., vol. 5041. Springer-Verlag, 2009, in press.

[52] M. Fallahpour, D. Megías, and M. Ghanbari, "Subjectively adapted high capacity lossless image data hiding based on prediction errors," submitted.