Reversible watermarking scheme with payload and signal robustness for audio signals

M. Alejandra Menéndez Ortiz, Claudia Feregrino-Uribe, José J. García-Hernández

Technical Report No. CCC-15-006
December 2015

Luis Enrique Erro 1
Santa María Tonantzintla
72840, Puebla, México.

Reversible watermarking scheme with payload and signal robustness for audio signals

M. Alejandra Menéndez Ortiz[1], Claudia Feregrino Uribe[1], J. Juan García Hernández[2]

1. Coordinación de Ciencias Computacionales, INAOE
Luis Enrique Erro #1, Sta. Ma. Tonantzintla, Puebla, 72840, México
2. Laboratorio de Tecnologías de Información, CINVESTAV, Unidad Tamaulipas
Parque Científico y Tecnológico TECNOTAM – Km. 5.5 carretera Cd. Victoria-Soto La Marina,
Cd. Victoria, Tamps., 87130, México
E-mail: {m.menendez,cferegrino}@ccc.inaoep.mx, jjuan@tamps.cinvestav.mx

Abstract. Robust reversible watermarking schemes (RWS) allow the reconstruction of a host signal and the extraction of a watermark if no attacks occur, but in the presence of attacks they either: extract the watermark, or reconstruct the host signal. This research proposal focuses on a robust RWS for audio that can both extract the watermark and reconstruct the host audio even when attacks occur. In order to meet both properties, the scheme must select relevant characteristics of an audio signal, which should: be robust enough to survive a set of attacks, be small enough to fit within the audio signal, and contain enough information to reconstruct the host audio. Additionally, the embedding process must produce a distortion smaller than an established distortion constraint. The contributions are the design of a RWS with payload and signal robustnes, and a mechanism that selects relevant characteristics of audio signals. This robust RWS can be constructed: combining a RWS with signal robustness and a fragile RWS, or modifying a RWS with signal robustness in a way that a useful payload can be inserted into the watermarked audio. A proposed robust RWS was designed following the first approach of solution and the results obtained show that it has an average embedding distortion of 26.63 dB, and payload and signal robustness against content replacement. These results suggest that it is possible to design a RWS with payload and signal robustness for audio signals that meets the desired characteristics of this research.

Keywords: Reversible watermarking scheme, payload and signal robustness, signal reconstruction, audio signals, attacks

1 Introduction

Digital media such as video, audio and images, is easily transmitted, manipulated and commercialized through digital channels. However, given their facility of manipulation it is easier to copy, modify or distribute them in an illegal manner. These illegal actions are known as piracy and looking for a way to counteract them, the Digital Rights Management (DRM) systems were created. These systems allow to control and restrict the access to digital multimedia; they include encryption, conditional access, copy control mechanisms, and media identification and tracing mechanisms. Digital watermarking is a key technology in these systems and is used for copy control, and media identification and tracing [HR00].

Digital watermarking schemes insert a secret message into a host signal in a way that is imperceptible for a human observer but that can be recovered given an extraction algorithm. However, conventional watermarking schemes produce a distortion in the carrier signal that causes loss of data. There are applications in the medical and military field where it is imperative that the carrier signal does not suffer loss of data and in those applications conventional watermarking schemes are not suitable.

With that situation, reversible watermarking schemes (RWS) arose. These schemes can insert a secret message within a carrier signal and later the modifications suffered during insertion can be reversed in order to obtain the host signal. However, reversible watermarking schemes can only reconstruct the host signal if the watermarked version does not suffer any additional modifications, *i.e.* if the watermarked signal is not submitted to attacks. If a signal marked with a reversible watermarking scheme goes through a modification, then the reversibility of the system is lost and the host signal cannot be reconstructed.

Robust reversible watermarking schemes were created to compensate the drawback of the reversible watermarking schemes. There are two aspects of this problem that the robust reversible watermarking schemes tackle. First, works like the one proposed by De Vleeschouwer *et al.* [DDM03] can reconstruct the host signal and the secret message, like the rest of the reversible watermarking schemes, if no attacks occur; in case of attacks these schemes can extract the secret message but the host signal is lost. Another type of robust reversible watermarking schemes, like the one proposed by Zhang *et al.* [ZW08], are able to reconstruct the host image regardless of attacks; nontheless these schemes cannot insert a secret message.

Another solution for the problem of perfect reconstruction of a host image and a secret watermark, even in the presence of attacks, was proposed from the communications point of view. Works like the one proposed by Kalker and Willems [KW03] design a system where a host signal and a secret message can be reconstructed regardless of modifications suffered in the transmission channel. However, these systems are designed only for binary signals and are not suitable for practical watermarking applications.

To date there is no reversible watermarking scheme that can reconstruct a host signal and extract a secret message from a watermarked signal, whether the latter suffered attacks or not. This investigation seeks the design of a reversible watermarking scheme with payload and signal robustness for audio signals that is able to reconstruct a host audio and extract a hidden message from a watermarked audio that can be modified by a set of attacks. The embedding procedure of the proposed scheme should produce a distortion smaller than an established constraint.

Besides a reversible watermarking scheme that satisfies the characteristics previously described, the contribution of this investigation is a mechanism that selects relevant characteristics of an audio signal and constructs control data based on those characteristics; the control data should be robust enough to survive modifications caused by a set of attacks, must be small enough to be embedded into the audio signal and provide enough information in order to reconstruct the host audio.

To design the reversible watermarking scheme of interest in this research, two possible approaches have been considered. The first is the combination of a reversible watermarking scheme with signal robustness and a fragile reversible watermarking scheme. The second approach is to modify a reversible watermarking scheme with signal robustness in a way that it can insert a useful payload. This modification can be the reduction of the control data or the embedding distortion.

Considering the first approach as the starting point in this proposal, a reversible watermarking scheme with payload and signal robustness is designed. The results obtained with this proposed scheme show its robustness against the content replacement attack and suggest that it is possible to design a reversible watermarking scheme with payload and signal robustness for audio signals that meets the described characteristics.

The rest of this document is organized as follows: section 2 briefly describes the theoretical background of the research and analyses the principal related works; section 3 gives the justifications to follow this line of research and describes the problem and its elements; in section 4 the objectives of the investigation are given, along with the methodology and the work plan; section 5 presents the experiments and results obtained with the proposed approach, which suggest that it is possible to design a reversible watermarking scheme with payload and signal robustness for audio signals; finaly the conclusions of this work are presented in section 6.

2 Preliminaries

2.1 Digital watermarking

Digital watermarking schemes are designed to hide data into digital media, in such a way that a human observer cannot identify the hidden data neither the modifications in the digital content and those schemes must provide a computer algorithm that can detect and/or extract the data originally hidden. A digital watermark is a transparent and invisible information pattern that is inserted into a digital content (such as audio, video or images) with a given insertion algorithm. The watermarks are related to the media itself and they can be used to identify the owner of a song, provide aditional information like artist, album, year of release, among other applications [Sei05,CMB$^+$08].

Digital watermarking schemes must meet the following properties [CMB$^+$08,Lu04]:

- **Embedding effectiveness.** The effectiveness of a watermarking scheme is the probability that the output of the insertion process will be marked. For example, an audio is considered to be marked if the detection process finds a watermark within it.
- **Fidelity.** The fidelity of a watermarking scheme is the perceptual similarity between an original (not watermarked) audio and a watermarked one. This perceptual similarity can be measured by an statistical metric, that will fall in one of two categories: difference metrics or correlation metrics. As the name indicates, *difference metrics* measure the difference between the original audio X and the watermarked audio Y. The most common difference metric is the *signal to noise ratio* (SNR). The SNR is usually expressed in decibels and is given by the following formula [Lu04]:

$$\text{SNR(dB)} = 10log_{10}\frac{\sum_n X_n^2}{\sum_n (X_n - Y_n)^2} \tag{1}$$

where X_n corresponds to the n^{th} sample of the original audio X and Y_n is the n^{th} sample of the watermarked audio Y. This quality measure reflects the distortion that a watermark imposes over a signal. Although an acceptable noise level depends on the application and the characteristics of the original audio, it is desired that the distorted audio has a SNR value of 35 dB. Another difference metric is the *peak signal to noise ratio* (PSNR) that measures the maximum signal to noise ratio found on an audio signal. The PSNR is given by the formula [Lu04]:

$$\text{PSNR(dB)} = N \times \frac{\text{MAX}^2}{\sum_n^N (X_n - Y_n)^2} \tag{2}$$

where N is the total number of samples in the audio signals, MAX is the maximum possible value of a sample, X_n corresponds to the n^{th} sample of the original audio X and Y_n is the n^{th} sample of the watermarked audio Y.

The *correlation metrics* measure the distortion based on the statistical correlation between the original and the watermarked audio. The *normalized cross-correlation* (NC) and the *correlation quality* (CQ) are two metrics that fall into this category.

When a metric that gives results in decibels is used, it is difficult to make comparisons because they use a logarithmic scale. It is simpler to present results using a normalized quality rating. The ITU-R Rec.500 quality rating gives a quality rating on a scale from 1 to 5. Table 1 presents the rating scale along with the quality level. This quality rating is calculated using the formula [Lu04]:

$$Quality = F = \frac{5}{1 + \text{Norm} \times \text{SNR}} \tag{3}$$

where Norm is a normalization constant and SNR is the measured signal to noise ratio. The result corresponds to the fidelity F of the watermarked audio.

Table 1: ITU-R Rec.500 quality rating

Rating	Description	Quality
5	Imperceptible	Excellent
4	Perceptible, not annoying	Good
3	Slightly annoying	Fair
2	Annoying	Poor
1	Very annoying	Bad

An objective mesure to evaluate audio quality is the *objective difference grade* (ODG). The objective measurement algorithms model the listening behavior of humans; their output is a number that describes the audibility of the introduced distortions. The objective measurent method of the perceived audio quality (PEAQ) is an international standard, ITU-R BS.1387, that follows the architecture given in Figure 2.1. This algorithms compares the difference between a reference signal (original) and a test signal (watermarked); both signals are processed by an auditory system that calculates an estimate of the audible components of the signal. These components can be considered as the representation of the signals in the human auditory system. The internal representation is related to the masked threshold, which in turn is based on a psychoacoustic model. From these two internal representations an audible difference is calculated and the cognitive model calculates the ODG value from the audible difference [CS08].

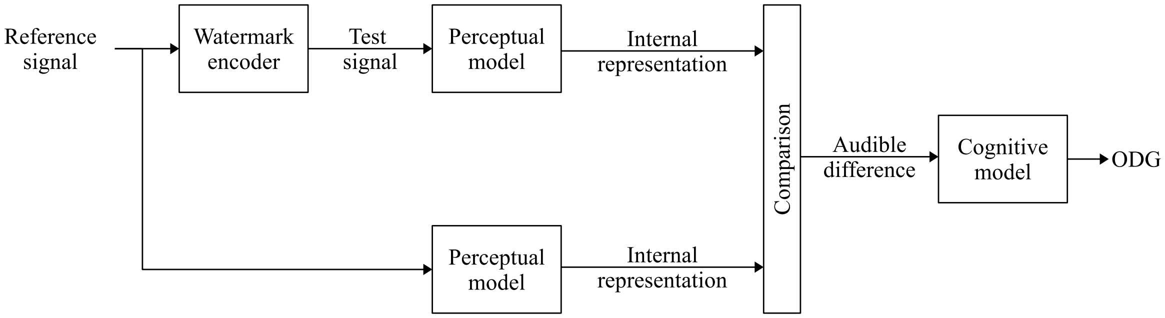


Fig. 2.1: Architecture for objective quality measurement of audio signals.

- **Data payload.** The data payload refers to the number of bits that a watermark encodes within a unit of time or within a signal. A scheme that encodes N bits can be used to embed 2^N messages. In audio, the data payload is measured by the number of bits that can be encoded in one second, i.e., the number of *bits per second* (bps).
- **Blind or informed detection.** In copyright protection and transaction-tracking applications the detection algorithms can have access to the unwatermarked audio in order to extract the message, although there may be cases where the detector only uses information derived from the original audio; these are known as *informed detectors*. In copy control applications the detector does not have access to the original audio when extracting the message; these are called *blind detectors*.
- **False positive rate.** A *false positive* is the detection of a watermark in an audio that does not actually contain one. A false positive rate is the number of expected false positives detections that occur in a given number of runs of the detector. The false positive rate of a scheme must be very low when detecting a watermark.

- **Robustnesss.** The robustness is the ability to detect a watermark after a watermarked audio has been subjected to a common signal processing operation (non intentional attack) or an intentional attack. Some examples of non intentional attacks for audio are MP3 compression, additive noise, resampling, filtering, analog-to-digital conversion (A/D), digital-to-analog conversion (D/A), among others. There also exist some processes where attackers intentionaly to remove the watermarks or intentionally analize the watermarked audio in order to estimate the embedded watermark.

Depending on the application of the watermarking scheme some properties might be irrelevant or have a broader tolerance. Watermarking schemes are not designed in a way that all the properties comply the best results, but rather the most important ones are exploited in order to be better suited for certain applications.

2.2 Conventional and reversible watermarking

A conventional watermarking scheme consists of two processes: embedding and extraction. In the embedding process a secret message M is hidden in a host signal X (an original audio, for example), obtaining in that way a watermarked signal Y. When this watermarked signal is transmitted over a communication channel, it may suffer intentional or non intentional attacks. Therefore, the extraction process may receive a watermarked Y or an attacked $\hat{Y}$ signal . The extraction process can have access to the host signal or not in order to retrive a message M', also it may or may not retrieve a signal X'. In the ideal scenario, where no attacks occurr during transmission, the recovered message M' is equal to the embedded message M and the recovered signal X' is very similar to the host signal X. Figure 2.2 shows the elements of a conventional watermarking scheme.

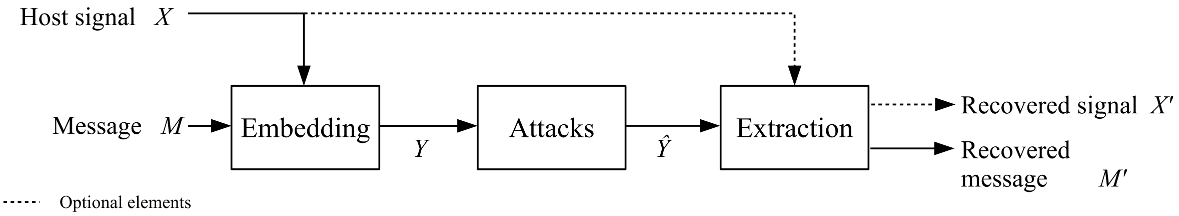


Fig. 2.2: Elements in a conventional watermarking scheme.

However, host signals used to carry payload in conventional watermarking schemes always suffer some level of degradation. Although this degradation can be controlled with a threshold, it is inevitable that these modifications occur. The embedding process of conventional schemes modifies the host signal in such a manner that the original values are lost. The extraction process recovers the hidden data and even though the retrieved signal is very similar to the original one, it is not *exactly* the same because of the degradation introduced during the embedding process.

Some applications like teleconferencing [BdB03], navigating and alerting for the blind [MGL98], warning and supporting for traffic situations in vehicles [CFNS06,PLR09] or aviation [Beg06] use high-quality audio. In some cases, like in the commercial field, it is desired that these high-quality audios do not suffer from loss of data. However, in the military and medical fields, applications like treatment of voice disorders or in systems for aviation warning, it is essential that the audios utilized do not suffer any kind of degradation.

Assume a medical application in telerehabilitation for voice and speech disorders [THR13], where a doctor receives an audio with a patient's speech, analyses it and diagnoses a treatment. A watermarking scheme can be used to insert additional information about the patient's current conditions, so there is no need to send that data in an additional file. If the additional data was embedded into the speech using a conventional watermarking scheme, when the extraction process retrieves the watermark, there will be loss of data in the recovered speech. In such scenario a reliable diagnosis cannot be made, because the doctor might have a speech with a lower quality than the necessary to evaluate the voice or speech of the patient. Even though conventional watermarking schemes can be limited to a very low distortion with a quality constraint, the host signal will not be *completely* recovered.

This example helps to illustrate that conventional watermarking schemes are not sufficient for certain applications. With this situation, some modifications were made to the conventional watermarking schemes and reversible watermarking arose. Reversible watermarking schemes have the advantage that the host signal can be reconstructed after the watermarks are recovered, contrary to conventional watermarking where the host signal is lost and only a similar version of the signal can be retrieved. Figure 2.3 shows the elements in a reversible watermarking scheme.

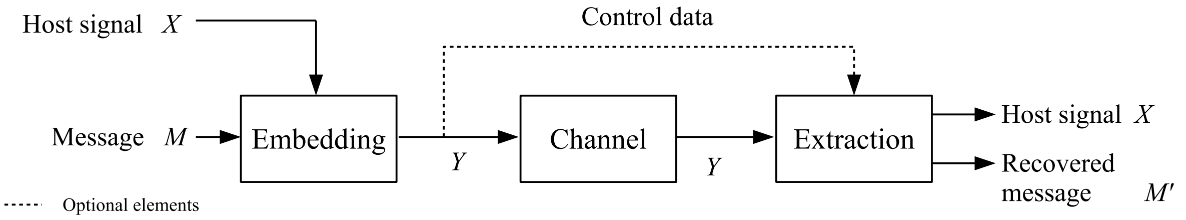


Fig. 2.3: Elements in a reversible watermarking scheme.

In recent years, proposed reversible watermarking schemes tried to improve payload capacity and imperceptibility. Because reversible watermarking schemes need control information to be able to restore the host signal after extraction, the actual space for data watermarking is significantly reduced. This is a challenging situation, thus many research groups have tried to tackle this problem. A consequence of the embedding process is the signal degradation; no matter if the embedding process is part of a conventional watermarking scheme or a reversible one, watermark insertion will modify the host signal, thereby creating signal degradation. Watermark imperceptibility is another challenge in reversible watermarking, because the design of an embedding procedure that minimizes perceptual impact is not a trivial task. Many researchers have worked in the design of embedding procedures that allow higher payload embedding capacity, while reducing perceptual impact at the same time.

2.3 Robustness in reversible watermarking

Another research line in reversible watermarking schemes is their robustness to attacks. This robustness property has been rarely explored and these efforts began just a decade ago. So far, robustness in reversible watermarking has been approached from the following points of view:

Payload robustness. In this robustness scenario, both the embedded watermarks and the host signal can be recovered only if no attack occurred in the communication channel. When attacks do occur in this channel, only the embedded watermarks can be retrieved, and there is no guarantee that the host signal can be reconstructed (Figure 2.4). In an attack situation, the recovered signal may be very similar to the host one, nonetheless it is not exactly the same, thus in this situation there is no reversibility.

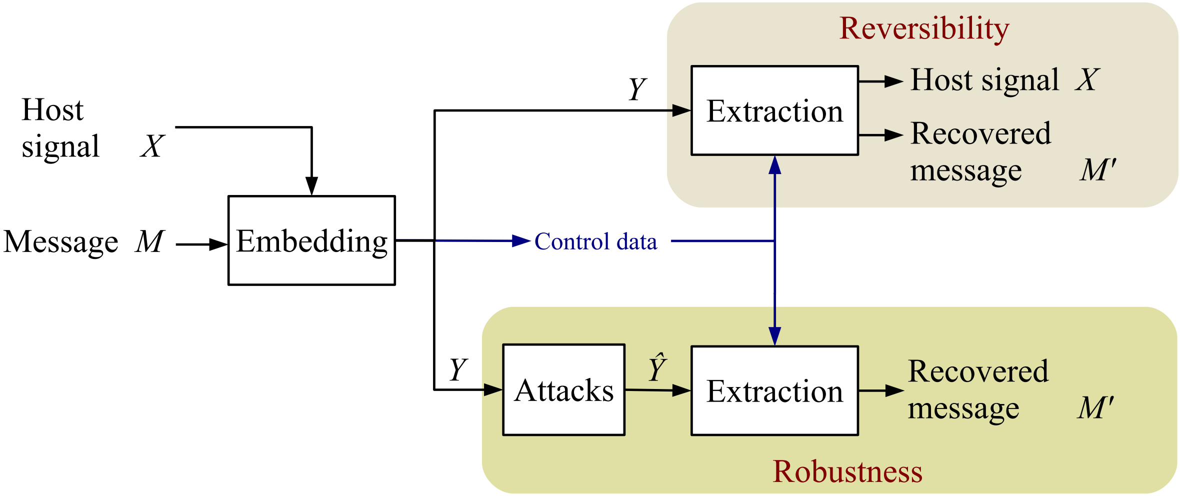


Fig. 2.4: Elements in a reversible watermarking scheme with payload robustness.

Depending on the robustness that the watermarks present, these schemes can be further classified as semi-fragile or robust. The watermarks in the semi-fragile schemes resist only unintentional attacks, like slight compression; on the other hand, the watermarks in the robust schemes should be able to survive intentional attacks, like signal processing operations. The former were the first efforts to preserve the embedded watermarks after some kind of processing was applied to the watermarked signal.

The first semi-fragile reversible watermarking scheme found in the literature is the one proposed by De Vleeschouwer *et al.* in 2003 [DDM03]; their scheme works with images in the spatial domain and resists JPEG compression; however, the watermarked images suffer from salt-and-pepper noise. Ni *et al.* [NSA$^+$04,NSA$^+$08] proposed a scheme where they solve the problem of salt-and-pepper in the previous scheme; this scheme also works with images in the spatial domain and resists JPEG and JPEG2000 compression; nonetheless, this scheme has short embedding capacity. Zou *et al.* [ZSN04,ZSNS06] presented another scheme that solves the salt-and-pepper issue; they use images in the integer wavelet transform (IWT) domain and their scheme resists JPEG2000 compression, but the embedding capacity is also little. Wu *et al.* [Wu07] proposed a scheme that works in the IWT domain and resists JPEG compression. Finally, Kim *et al.* [KLSL09] designed a scheme that utilizes images in the spatial domain and resists JPEG compression. Table 2 depicts a summary of these schemes.

The first robust reversible watermarking schemes appeared in 2007. Chrysochos *et al.* [CFSX07] proposed a scheme that works with images in the spatial domain and is robust to various attacks, such as flipping, rotation, up-sizing, increasing aspect ratio, cropping, drawing, among others; however, the embedding capacity is low. Coltuc and Chassery [CC07] presented a scheme that works in the integer transform domain (ITD), is robust against cropping. Coatrieux *et al.* [CMHR07] proposed a scheme that works with magnetic resonance images in spatial domain and is robust against JPEG compression. Gao and Gu [GG07] introduced a scheme that works in the IWT domain and has robustness to cropping and salt-and-pepper noise.

Saberian *et al.* [SAM08] proposed a scheme for images and signals in the spatial and temporal domain, respectively, besides, both images and signals can be processed in the transform domain; this

Table 2: Reversible watermarking schemes with semi-fragile payload.

Reference	Author	Year	Domain	Host type	Attacks
[DDM03]	De Vleeschouwer	2003	Spatial	Image	JPEG
[NSA+04]	Ni	2004	Spatial	Image	JPEG, JPEG2000
[ZSN04]	Zou	2004	IWT	Image	JPEG2000
[ZSNS06]	Zou	2006	IWT	Image	JPEG2000
[Wu07]	Wu	2007	IWT	Image	JPEG
[NSA+08]	Ni	2008	Spatial	Image	JPEG, JPEG2000
[KLSL09]	Kim	2009	Spatial	Image	JPEG

scheme is robust against the addition of white Gaussian noise (AWGN). Gu *et al.* [GHGC09] presented a scheme in the wavelet domain that is robust against JPEG compression. Chang *et al.* [CLY09] introduced a scheme that works with images in the discrete cosine transform (DCT) domain and is robust to blurring, brightness, contrast and cropping, among others. Yang *et al.* [YLH10] proposed a method in the IWT domain that is robust against brightness, JPEG and JPEG2000 compression, cropping and inversion. Tsai et al. [TTL10] presented a scheme in the discrete wavelet transform (DWT) domain that is robust to JPEG compression, AWGN, salt and pepper noise, scaling and blurring, among others. Zeng *et al.* [ZPP10] introduced a scheme that uses images in the spatial domain and is robust against JPEG compression. Gao *et al.* [GAY+11] also presented a scheme that works with images in spatial domain and is robust to JPEG compression. An *et al.* proposed three different schemes en 2012; two of them [AGY+12], [AGYT12] work with images in spatial domain and both are robust against JPEG and JPEG2000 compression, and additive AWGN. Their third scheme [AGL+12] uses images in wavelet domain and is robust against JPEG and JPEG2000 compression, and additive AWGN as well. Table 3 presents a summary of these schemes.

Signal robustness. With this kind of robustness, the host signal can be reconstructed whether attacks occurred in the transmission channel or not. Nonetheless, these schemes cannot embed useful payload. In other words, the whole embedding capacity is used to insert control data and no watermarks at all. The control data may contain a compressed version of the signal or significant characteristics of the signal that help to the reconstruction process. These watermarking schemes can be further classified as those that obtain an approximate version of the signal and those that achieve a perfect reconstruction of the signal.

Figure 2.5 shows the elements in a watermarking scheme with approximate signal reconstruction. This type of schemes can detect tampered regions of a signal and try to reconstruct the tampered regions using the embedded control data. Although this reconstructed signal may be similar to the original signal, it is not a lossless version of the host signal.

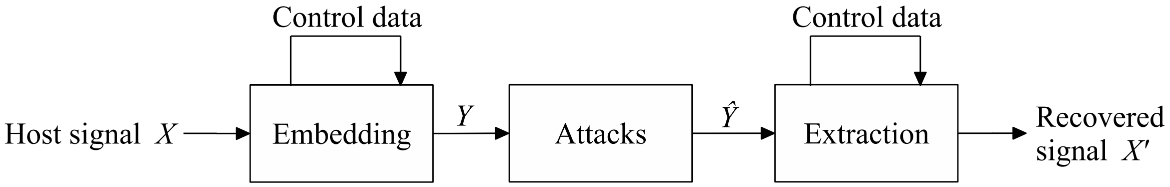


Fig. 2.5: Elements in a reversible watermarking scheme with approximate signal reconstruction.

Table 3: Reversible watermarking schemes with robust payload.

Reference	**Author**	**Year**	**Domain**	**Host type**	**Attacks**
[CFSX07]	Chrysochos	2007	Spatial	Image	Flipping, rotation, translation, up-sizing, cropping, increasing aspect ratio, scattered tiles
[CC07]	Coltuc	2007	Integer	Image	Cropping
[CMHR07]	Coatrieux	2007	Spatial	Image	JPEG
[GG07]	Gao	2007	IWT	Image	Cropping, salt-and-pepper noise
[SAM08]	Saberian	2008	Spatial/ Temporal Transform	Image, Audio	AWGN
[GHGC09]	Gu	2009	Wavelet	Image	JPEG
[CLY09]	Chang	2009	DCT	Image	Blurring, brightness, contrast, cropping, equalization, noise, JPEG, scaling, sharpening
[YLH10]	Yang	2010	IWT	Image	Brightness, JPEG, JPEG2000, cropping, inversion
[TTL10]	Tsai	2010	DWT	Image	JPEG, AWGN, salt and pepper noise, scaling, blurring, brightness, darkness, sharpen, equalization, cropping, painting
[ZPP10]	Zeng	2010	Spatial	Image	JPEG
[GAY$^+$11]	Gao	2011	Spatial	Image	JPEG
[AGY$^+$12]	An	2012	Spatial	Image	JPEG, JPEG2000, AWGN
[AGYT12]	An	2012	Spatial	Image	JPEG, JPEG2000, AWGN
[AGL$^+$12]	An	2012	Wavelet	Image	JPEG, JPEG2000, AWGN

Table 4 presents the watermarking schemes with approximate signal reconstruction. The first works that recovered a signal after this was subjected to attacks were proposed by Fridrich and Goljan in 1999 [FG99a,FG99b]. From these works, many schemes have been proposed to date, some of them modify the domain where the embedding takes place, others improve the compression method to calculate the control data to be embedded in the signal itself. Now some relevant works will be breafly described.

Table 4: Watermarking schemes with signal approximate reconstruction.

Reference	Author	Year	Domain	Host type	Tamper detection	Tamper correction	Attacks
[FG99a]	Fridrich	1999	DCT	Image	✓	✓	Content replacement, random noise
[FG99b]	Fridrich	1999	DCT	Image	✓	✓	Content replacement, random noise
[Mob00]	Mobasseri	2000	DCT	Video	✓	✓	MPEG
[ME01]	Mobasseri	2001	Spatial/ Temporal	Video	✓	✓	Frame removal, frame insertion
[WC02]	Wu	2002	DCT	Image	✓	✓	Content replacement, bluring, sharpening, JPEG
[GCG$^+$02]	Gomez	2002	Temporal	Audio	✓	×	Insertion, deletion
[CSTS02]	Celik	2002	Spatial/ Temporal	Video	✓	✓	Frame rate conversion, frame dropping, frame insertion, content replacement
[SD03]	Steinebach	2003	Temporal	Audio	✓	×	Cropping
[CBC$^+$03]	Caldelli	2003	DWT	Image	✓	✓	Content replacement JPEG
[LHH05]	Lin	2005	Spatial	Image	✓	✓	—
[ZHM07]	Zhu	2007	Spatial	Image	✓	✓	Block replacement, filtering, noise, contrast modification
[ZHT$^+$07]	Zhao	2007	SLT	Image	✓	✓	Cut and paste, JPEG
[WC07]	Wang	2007	Spatial	Image	✓	✓	Collage, vector quantization
[HC07]	Hung	2007	Spatial	Image	✓	✓	Cropping, JPEG, content replacement
[HH07]	Hasan	2007	Spatial/ DCT	Image	✓	✓	Blind copy
[WT08]	Wang	2008	Spatial	Image	✓	✓	Content replacement
[JL08]	Jiang	2008	DCT	Image	✓	✓	Content replacement, adding text, block exchange, collussion, erasing
[HZC08]	He	2008	Spatial	Image	✓	✓	Content replacement
[CHW08]	Chen	2008	Temporal	Audio	✓	✓	Cropping
[KE09]	Karantonis	2009	DCT	Image	✓	✓	—
[HZT09]	He	2009	Spatial	Image	✓	✓	Content replacement, collage, constant average

Continues on next page

Reference	**Author**	**Year**	**Domain**	**Host type**	**Tamper detection**	**Tamper correction**	**Attacks**
[HAHH$^+$09]	Hassan	2009	Spatial/ Temporal	Video	✓	✓	Vector quantization, content replacement
[CCCK09]	Cheddad	2009	DWT	Image	✓	✓	—
[QQ10]	Qian	2010	DCT	Image	✓	✓	—
[QF10]	Qian	2010	DCT	Image	✓	✓	—
[MNKNMPM10]	Mendoza-Noriega	2010	DCT	Image	✓	✓	JPEG
[KSD10]	Korus	2010	DWT	Image	✓	✓	Blurring, JPEG
[IHSO10]	Iwata	2010	DCT	Image	✓	✓	Content replacement
[HAHM$^+$10]	Hassan	2010	Spatial	Image	✓	✓	Vector quantization
[HAHH$^+$10]	Hassan	2010	Spatial	Image	✓	✓	Vector quantization
[CRMH10]	Cruz	2010	DCT	Image	✓	✓	JPEG
[ZQRF11]	Zhang	2011	DCT	Image	✓	✓	Content replacement
[SQL$^+$11]	Shi	2011	Spatial/ Temporal	Video	✓	✓	Content replacement
[MNKMM11]	Mendoza-Noriega	2011	IWT	Image	✓	✓	Salt and pepper, drawing
[LWMZ11]	Li	2011	DCT	Image	✓	✓	Collage, content tampering
[KJR11]	Korus	2011	DWT	Image	✓	✓	—
[QCC12]	Qin	2012	NSCT	Image	✓	✓	Drawing
[KD12]	Korus	2012	Spatial	Image	✓	✓	—
[HCT$^+$12]	He	2012	Spatial	Image	✓	✓	Collage, constant average
[BSLN12b]	Bravo-Solorio	2012	Spatial	Image	✓	✓	Cropping
[AMAC12]	Ahsan	2012	DWT	Image	✓	✓	—
[SQY$^+$13]	Shi	2013	Spatial/ Temporal	Video	✓	✓	—
[KD13]	Korus	2013	Spatial	Image	✓	✓	—

As previously mentioned, the works of Fridrich and Goljan [FG99a,FG99b] appeared in 1999 and were the first to be able to reconstruct an image after some malicious operation was applied to the watermarked signal. Their schemes utilized the DCT to embed in this domain the compressed version of the image into itself. In 2000 Mobaseri [Mob00] proposed the first scheme for video signals and it was a modified version of the MPEG (Moving Picture Experts Group) compression standard. In 2002 Gomez *et al.* [GCG$^+$02] proposed the first scheme for audio signals, it embedded the watermarks in the temporal domain and the scheme was only able to detect the places where the audio had been modified but could not correct these modifications. In 2008 Chen *et al.* [CHW08] proposed the first scheme for audio signals that was able to correct, with a certain degree, the modifications imposed by cropping attack. Recent works like the ones proposed by Qin *et al.* [QCC12], and Korus and Dziech [KD12] improve the quality of the reconstructed image after it has been subjected to attacks. But even though these are high-quality images, they are not lossless versions of the original image.

Figure 2.6 shows the elements in a watermarking scheme with perfect signal reconstrucion. Like the schemes with approximate signal reconstruction, these can detect the regions where the signal was tampered and with the embedded control data, they can reconstruct the tampered regions. However, the reconstructed signal has exactly the same values that the ones in the host signal, *i.e.*, they achieve a perfect signal reconstruction.

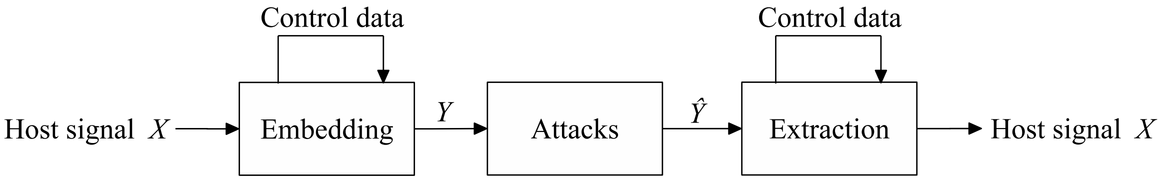


Fig. 2.6: Elements in a reversible watermarking scheme with perfect signal reconstruction.

Table 5 presents the watermarking schemes with perferct signal reconstruction capability. All of them were proposed for image signals and work in the spatial domain. The first method was proposed by Zhang and Wang in 2008 [ZW08]. This scheme is able to perfectly reconstruct the image after content replacement attack as long as the tampered areas are not too extensive. In 2011 Zhang *et al.* [ZWQF11] continued the scheme from [ZW08] where it can also reconstruct the image after content replacement attack as long as the tampered area is less than 24% of the image. In 2012 Bravo-Solorio *et al.* [BSLN12a] presented a scheme that can perfectly reconstruct an image after cropping attack, only if the tampered area is less than 25% of the image.

Table 5: Watermarking schemes with perfect signal reconstruction.

Reference	Author	Year	Domain	Host type	Tamper detection	Tamper correction	Attacks
[ZW08]	Zhang	2008	Spatial	Image	✓	✓	Content replacement
[ZWQF11]	Zhang	2011	Spatial	Image	✓	✓	Content replacement
[BSLN12a]	Bravo-Solorio	2012	Spatial	Image	✓	✓	Cropping

The drawback of both types of watermarking schemes is that they can reconstruct the signal only if the tampered area is not too extensive. If too many regions of the signal were corrupted, then the values of the compressed version that was originally embedded may be corrupted or lost during attacks.

Because of this not all the tampered regions may be reconstructed and if there were too many tampered regions, the whole image would be lost.

Payload and signal robustness. In this scenario, a watermarking scheme may reconstruct the host signal and the inserted payload no matter if attacks occurred or not in the transmission channel (Figure 2.7). So far, this problem has been addressed from the point of view of communications. It is possible to reconstruct the payload and the host signal after some theoretical attack within a symmetric binary transmission channel. However, even if some specific attack is established, this kind of scheme is not suitable for practical watermarking applications.

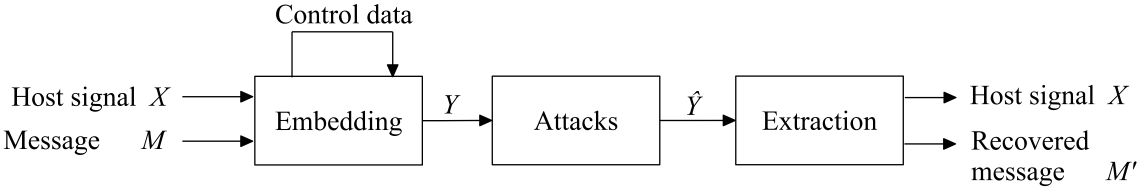


Fig. 2.7: Elements in a reversible watermarking scheme with payload and signal robustness.

Payload and signal robustness were first analyzed by Kalker and Willems in 2003 [KW03] and they gave a theoretical analysis of this situation. In their work, they present a scenario where a binary mark is embedded in a binary host signal, which in turn is transmitted through a symmetric binary channel. This transmission channel may cause a certain distortion to the watermarked signal and/or the embedded data. Kalker and Willems take the idea proposed by Fridrich *et al.* [FGD02], where they compress a host signal (image) in a lossless manner and concatenate a bitstream of auxiliary data. This auxiliary data contains the watermark and control data to reconstruct the host image. They extend this scheme to work in channels with attacks and they solve this by attaching error correcting codes to the auxiliary data. In this paper, only the theoretical foundations are given for an over-simplification of the problem and although this is a valid scenario for a communications problem, it does not satisfy the idea behind digital watermarking (where the watermarked signal must seem “intact” to the unaware observer).

The works by Willems and Kalker [WK04], Kotagiri and Laneman [KL05,KL06], Steinberg [Ste06]
[Ste08a][Ste08b][Ste09], Sumszyk and Steinberg [SS09], and Zhang *et al.* [ZCY11] continue the theoretical analysis given by Kalker and Willems, trying to improve the compressor, thus achieving higher theoretical payload capacities. In their work of 2012, Zhang *et al.* [ZCY12] proposed a code construction that enhances payload capacity and gave an example of how to improve a histogram shifting method by including their codes. This modified histogram shifting method only supports binary images. In 2013, Zhang *et al.* [ZHLY13] extended their codes to gray-scale signals and modified two histogram shifting methods to include their codes for gray-scale images. These modifications enhanced the payload capacity given a distortion constraint; however, only the distortion due to the embedding process is considered, not the distortion due to attacks. Figure 2.8 depicts a summary of these works and their most important characteristics.

As it can be seen, none of the works analyzed so far propose a reversible watermarking scheme robust against malicious attacks, designed for non-binary host signals. Some works have tackled the problem when malicious attacks occur in the transmission channel by converting the non-binary host signal into a binary host signal and then applying the existing methods. Nonetheless, reversible

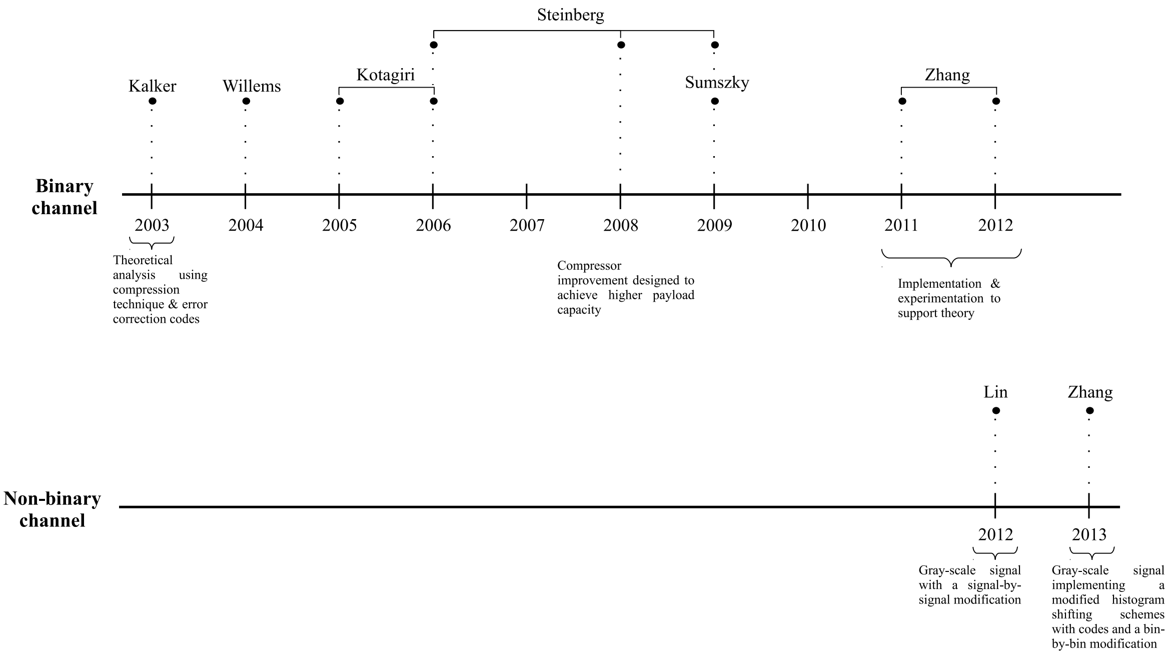

Steinberg
Kalker
Willems
Kotagiri
Sumszky
Zhang
Binary channel
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
Theoretical analysis using compression technique & error correction codes
Compressor improvement designed to achieve higher payload capacity
Implementation & experimentation to support theory
Lin
Zhang
Non-binary channel
2012
2013
Gray-scale signal with a signal-by-signal modification
Gray-scale signal implementing a modified histogram shifting schemes with codes and a bin-by-bin modification

Fig. 2.8: Chronology of the payload and signal robustness works.

schemes that are natively designed for non-binary host signals and that can survive malicious attacks have not been proposed yet. The design of such a scheme remains an open problem.

The design of a reversible watermarking scheme with payload and signal robustness is not a trivial task because of the following issues:

- The watermarks should be robust enough so that the extraction process can recover them even after distortions occur, both due to the embedding process and due to malicious attacks. But, besides robustness the watermarks should be, at the same time, transparent enough so that the user cannot note their presence, *i.e.*, they should be robust and imperceptible.
- The host signal must be recovered in the extraction process, independently of malicious attacks. That is, the extraction process should be able to compensate the malicious attacks, counterbalancing the distortions suffered by the host signal because of both the embedding process and the channel attacks. It is not a trivial task to be able to detect which attack or attacks occurred, given a set of possible attacks, all of which have a similar probability of occurrence. But even under the assumption that the extraction process is able to identify the attack or attacks that took place during transmission, it is hard to know the exact location in the signal where those modifications happened.
- There must be a mechanism in the embedding process that grants a balance between the robustness and the imperceptibility that the watermarks need.
- There must also be a way in the embedding process to decide which additional data should be inserted in the host signal, in such a way that the extraction process may be able to reconstruct the host signal. This decision should take into account that apart from embedding distortions, there could be distortions due to malicious attacks. So the embedding process should be able to foresee the attacks that would happen during transmission and the corresponding control data to repair the damage.

A discussion of the robustness presented in current reversible watermarking schemes is detailed below.

2.4 Discussion

All three robustness scenarios are challenging and may lead to interesting research lines; however reversible watermarking schemes with payload and signal robustness are far more desirable for real applications. For practical applications, the assumption made by conventional (not robust) reversible watermarking schemes that no attacks will occur is very unlikely.

Let's take back the example of the telerehabilitation for voice and speech disorders where additional information about the patient's current condition is going to be embedded as a watermark. But this time, let's suppose that the watermarked speech is too large and it must be compressed before transmission. In this case, a reversible watermarking scheme with payload robustness may extract the additional information embedded, but the original speech will be lost, because of the fragile nature of the signal in this kind of schemes. So, reversible watermarking with payload robustness would be useless for this case. Now, let's assume that a reversible watermarking scheme with signal robustness is used. In this case, the compressed speech can be transmitted and the original speech can be reconstructed in the receiver side; however, the scheme does not have space for payload insertion, so they will not be able to get the additional information within the same signal (like the name of the patient or his or her evolution to the treatment). So reversible watermarking with signal robustness is neither useful for this situation. Only a reversible watermarking scheme with payload and signal robustness would satisfy the necessities in this scenario. In real life applications, compression along with other modifications are very common and watermarking schemes should take this into consideration.

Schemes with payload or signal robustness may be useful for a certain type of applications, such as authentication for the former and tamper detection for the latter. However, those applications more similar to real life ones are very much likely to need robustness in both payload and signal. Nonetheless, the current schemes that deal with payload and signal robustness exist for binary hosts and if there is the need to transmit a watermarked non-binary signal under a noisy channel, where attacks may occur, it must be transformed into a binary signal to then apply the existing methods. However, as mentioned before, this strategy does not satisfy the idea behind watermarking applications; because in a watermarking scenario, the watermarked signal should not seem different from the original one. If a user observes the transmission channel and finds a signal that was converted to a binary one, the user would only see a sequence of compressed bits that do not resemble at all the original non-binary image. And the whole idea behing watermarking would be lost.

So, it can be seen that a situation like the one presented in the example above does not currently have a solution with any existing reversible watermarking schemes. There is the necessity of a reversible watermarking scheme that is able to perfectly reconstruct a signal and extract a hidden watermark from a non-binary signal, even after the watermarked signal was transmitted in a noisy channel, where attacks may or may not have occurred. This scheme should also take into consideration that the hidden data should not be noticeable for a human observer, so the embedding process should take into consideration degradation due to the embedding procedure and the extraction process must take into consideration degradations due to both embedding and attacks.

The brief review given in the subsection above, of the current situation in reversible watermarking includes schemes designed for images or theoretical analyses for signals in general, because those are the only efforts made so far; although this research focuses on the design of a reversible watermarking scheme with payload and signal robustness that utilizes audio signals. The existing works will be studied in order to identify key characteristics or ideas that will later be incorporated in the proposed scheme. The inclusion of these previous ideas to a new scheme might seem an unimportant contribution; however, this task includes more than just a simple translation from a two-dimensional to a one-dimensional plane (from image to audio). The current schemes must be thoroughly studied and their fundamental ideas must be completely understood in order to isolate the general strategy that solves the problem. Later, that general strategy must be adapted to satisfy the restrictions imposed by the characteristics of audio signals.

In the next section, the motivation of this work will be given along with the definition of the problem to be approached in this research.

3 Motivation

3.1 Motivation

As mentioned in section 2, some applications like teleconferencing [BdB03], navigating and alerting for the blind [MGL98], warning and supporting for traffic situations [CFNS06,PLR09,Beg06], among others, use high-quality audio signals. In real life applications it is highly probable that an audio will suffer modifications during its transmission. However, as it has been seen in the previous section, reversible watermarking schemes with payload robustness will only be able to extract the embedded watermarks in case of attacks; reversible watermarking schemes with signal robustness will not be able to insert aditional information into the audio; and reversible watermarking schemes with payload and signal robustness are only designed for binary signals, and converting the non-binary signal to a binary one would break the paradigm of digital watermarking.

From this, it is clear that currently no solution exists that solves the problem of a reversible watermarking scheme with payload and signal robustness for non-binary signals in general, and for audio signals in particular. A detailed specification of the problem that will be approached in this investigation is given below.

3.2 Problem definition

Applications that require transmission of high-quality audios along with additional data require the following characteristics (Fig. 3.1):

- The sender side must embed a secret message M, into a host signal X. This message is related to that signal, and both message and signal must be transmitted through a channel where:
  - the host signal is a non-binary one,
  - and the secret message must be embedded into the signal in such a way that the watermarked signal Y, has a distortion due to embedding that does not exceed an α constraint.
- The transmission channel is a noisy non-binary one, where a set of attacks may occur; these attacks will impose a distortion (distortion due to attacks, β) to the watermarked signal, resulting in an attacked signal $\hat{Y}$.
- The receiver side should be able to extract the embedded message M' and counteract the distortion due to embedding (α) and the distortion due to attacks (β) in order to reconstruct a signal that has the same values as the host signal X.

A system that meets all the previous restrictions does not currently exist. The design of a reversible watermarking scheme that satisfies these characteristics remains as an open problem and is the focus of this doctoral research. The next section details the scope of this research.

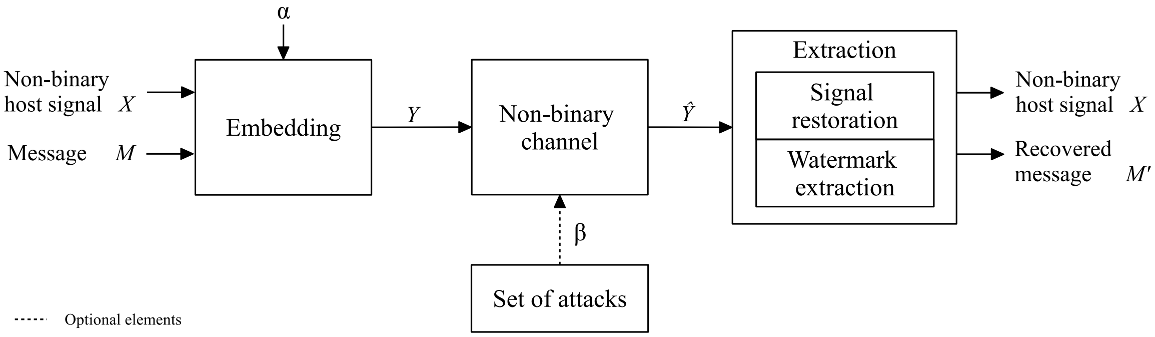


Fig. 3.1: Elements in the problem situaton.

4 Proposal

This section describes the elements of this proposal and a general outline on how the problem will be addressed.

4.1 Research questions

- Is it possible to design an embedding process that is able to insert a secret message and control data into an audio signal in such a way that the watermarked audio meets a distortion due to embedding constraint α?
    - Is it possible to design a mechanism that selects the important characteristicst of an audio signal to construct the control data of an embedding process in such a way that this control data helps an extraction process in the reconstruction of a host audio that suffered possible attacks?
    - Which are important characteristics in an audio signal that may survive a set of possible attacks?
    - Which is an acceptable distortion due to embedding constraint α?
- Which is a significant set of audio attacks that are commonly applied during transmission?
- Is it possible to design a robust mechanism that is able to extract a hidden watermark even after a set of attacks might be applied to the watermarked audio?
- Is it possible to design a mechanism that finds the locations in a watermarked audio where a set of attacks caused modifications?
    - Can this mechanism compensate those modifications that impossed a distortion due to attacks β, given the control data previously extracted?
- Is it possible to design a mechanism that is able to compensate the distortion due to embedding α?

4.2 General objective

Design a reversible watermarking scheme with payload and signal robustness that is able to extract a hidden watermark with an acceptable error probability for practical or commercial applications and can reconstruct a host audio signal even in the presence of a set of attacks. The embedding process of this scheme must produce a distortion lower than an α constraint.

4.3 Specific objectives

- Design a mechanism that is able to select relevant characteristics of an audio signal in order to construct control data that will be embedded into a host audio; those characteristics should be robust enough to survive a set of attacks.
- Determine an α constraint for an acceptable distortion due to embedding.
- Design an embedding process that inserts a watermark and control data into a host audio signal, meetting an α constraint.
- Select a set of audio attacks that are commonly applied during transmission.
- Design a watermark extraction mechanism that can recover a watermark and control data hidden in an attacked audio signal with low error probability.
- Design a signal restoration mechanism that is able to reconstruct a host audio signal, given an audio signal with distortion due to attacks β and distortion due to embedding α, and control data that has relevant characteristics of the host audio signal.

4.4 Methodology

Two main lines have been considered that might lead to a solution of the problem. Figure 4.1 presents an outline of these lines.

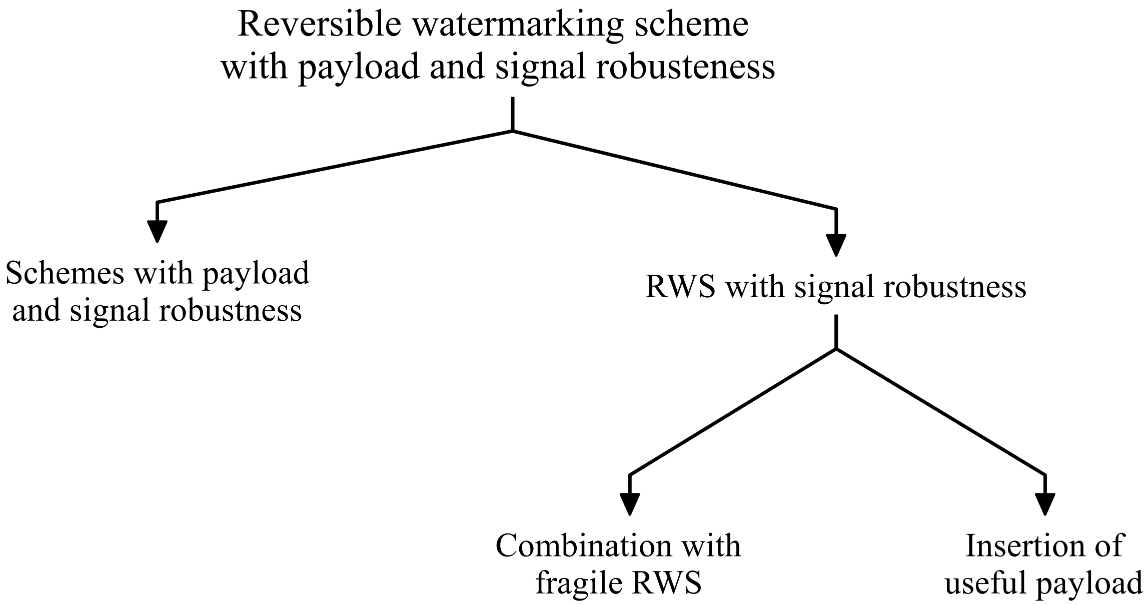


Fig. 4.1: Possible considered lines to solve the problem.

Line 1. Schemes with payload and signal robustness for binary signals. Following this line of solution, schemes with payload and signal robustness for binary signals would be modify to work with non-binary audio signals and a non-binary channel. However, this would first require a formal definition of the attacks and the creation of detailed models that determine their behavior. The theoretical analysis in this line would have to be extensive and although a solid foundation for future work would be established, a period of time longer than the available could be neccesary to state a proper theoretical background and develop a solution from there.

Line 2. Reversible watermarking schemes (RWS) with signal robustness. This line has been considered as the starting point in the proposed research. The idea is to take a reversible watermarking scheme with signal robustness and modify it in a way that useful payload can be robustly embedded along with control data. Based on this idea, two strategies (also depicted in Fig 4.1) have been considered:

2.A. Combination with fragile RWS. This strategy consists on isolate the general ideas from a reversible watermarking scheme with signal robustness and combine them with a fragile reversible watermarking scheme in order to design a new scheme with payload and signal robustness. The fragile scheme will allow to embed a watermark and control data to reconstruct the host audio signal; the scheme with signal robustness will allow to protect the watermarked audio against attacks. Given that the watermarked audio will be the same as the one in the embedding process, a fragile reversible extraction process can be utilized to extract the watermark and reconstruct the host audio signal. From now on, a scheme constructed with this strategy will be referred as a “type 1” scheme and an outline of its elements is depicted in Figure 4.2.

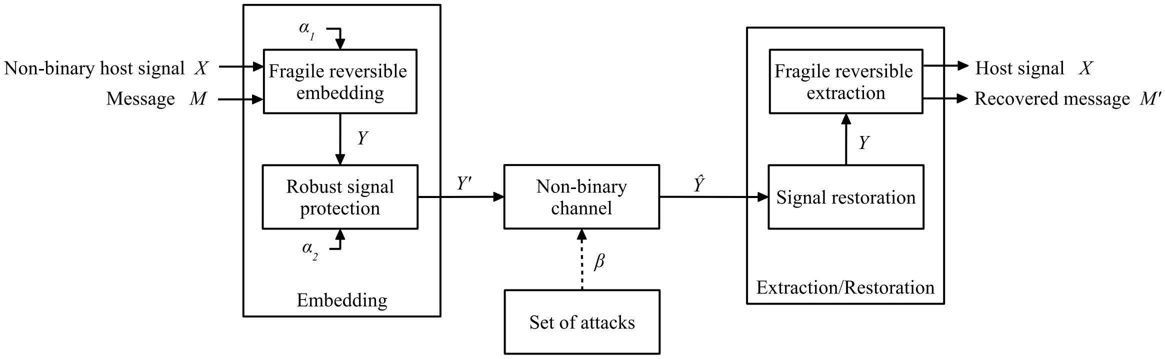


Fig. 4.2: Elements in a “type 1” scheme.

In a type 1 scheme, a fragile reversible embedding process inserts a secret message M into a non-binary host audio signal X, creating a watermarked audio Y that suffered an embedding distortion α_1. Y is protected with a robust signal protection process (based on a RWS with signal robustness) creating a protected watermarked audio Y' that suffered a distortion α_2. If Y' is transmitted through a noissy channel, a set of attacks may impose a β distortion, resulting in an attacked audio $\hat{Y}$. On the receiver side the watermarked audio Y is reconstructed with a signal restoration process (based on a RWS with signal robustness). Finally, a fragile extraction process can take the recovered watermarked audio Y to reconstruct the host audio signal X and extract a secret message M'.

2.B. Insertion of useful payload. The second strategy is to modify an existing reversible watermarking scheme with signal robustness in a way that it can robustly insert a useful payload, converting it into a reversible watermarking scheme with payload and signal robustness. From now on, a scheme designed with this second strategy will be referred as a “type 2” scheme. So far, two ideas have been considered to design a type 2 scheme:

i. Reduce perceptual impact of the reversible watermarking scheme with signal robustness. These schemes are currently designed for spatial domain. However, their perceptual impact might be reduced if the scheme is translated to the frequency domain, although a proper transform must be selected to achieve the desired improvement. If the perceptual impact is reduced, given a fixed amount of control data, then a useful payload can be embedded, reaching a similar perceptual distortion as in the original scheme, but achieving the goal of useful payload insertion.

ii. Improve the compresion method. These schemes construct their control data by compressing the image itself. If a lossless compression algorithm that allows to achieve a higher compression rate is selected, then the space that was used to insert control data can be used to insert useful payload.

The proposed methodology will incorporate the strategies described before to design a reversible watermarking scheme with payload and signal robustness for audio signals. Figure 4.3 presents a diagram with the methodology steps.

It is important to highlight that although this research focuses on the design of a reversible watermarking scheme with payload and signal robusteness for audio signals, the first approaches will be proposed for images. As can be seen in the strategies described before, the general idea is to take an existing scheme and modify it in a way that the payload and signal robustness is reached. However, the existing schemes are designed for images, so the initial approaches will also be designed for that type of media and modifications will be made to achieve the desired robustness, since the existing reversible watermarking schemes for audio signals do not present any kind of robustness. When the proposed scheme propertly solves the problem of robust insertion and reconstruction of a host image and a watermark, the scheme will be adapted to work with audio signals.

A translation from images to audio could seem a trivial endeavour, nonetheless it is more complicated than just rearranging a vector of audio samples into a matrix and a direct application of the method. Given that the first version of the scheme will be based on existing ones, and the latter are desgined to exploit the inherent characteristics of image signals, the proposed scheme will also exploit those properties, like spatial correlation between pixels (*i.e.* the relation between neighboring pixels), the bit depth (usually 8 bits) of each sample that affects the dynamic range that can be represented and the sensitivity of the human visual system (HVS) to a given range of frequencies, for example. When translating the scheme to work from images to audio signals it must be taken into consideration that the properties of audio are very different from the properties of images. For example, the correlation between audio samples exists in time (given that an audio is a sequence of samples that change over time) instead of the spatial correlation between image pixels; audio signals usually have a bit depth higher than the one for images (16 bits per sample for audio) and the dynamic range thant can be reperesented with those values is different from the dynamic range for images; the human auditory system (HAS) is sensitive to a different range of frequencies than the HVS.

It can be seen that a group of strategies must be followed in order to correctly translate the underlying ideas of the scheme for images to work for audio signals, given all the differences between their properties. A first strategy is to find existing works in the literature that have already sucessfully translated a watermarking scheme for images to a watermarking scheme for audio, identify the properties that they took into consideration and the procedures that they followed to make the transition.

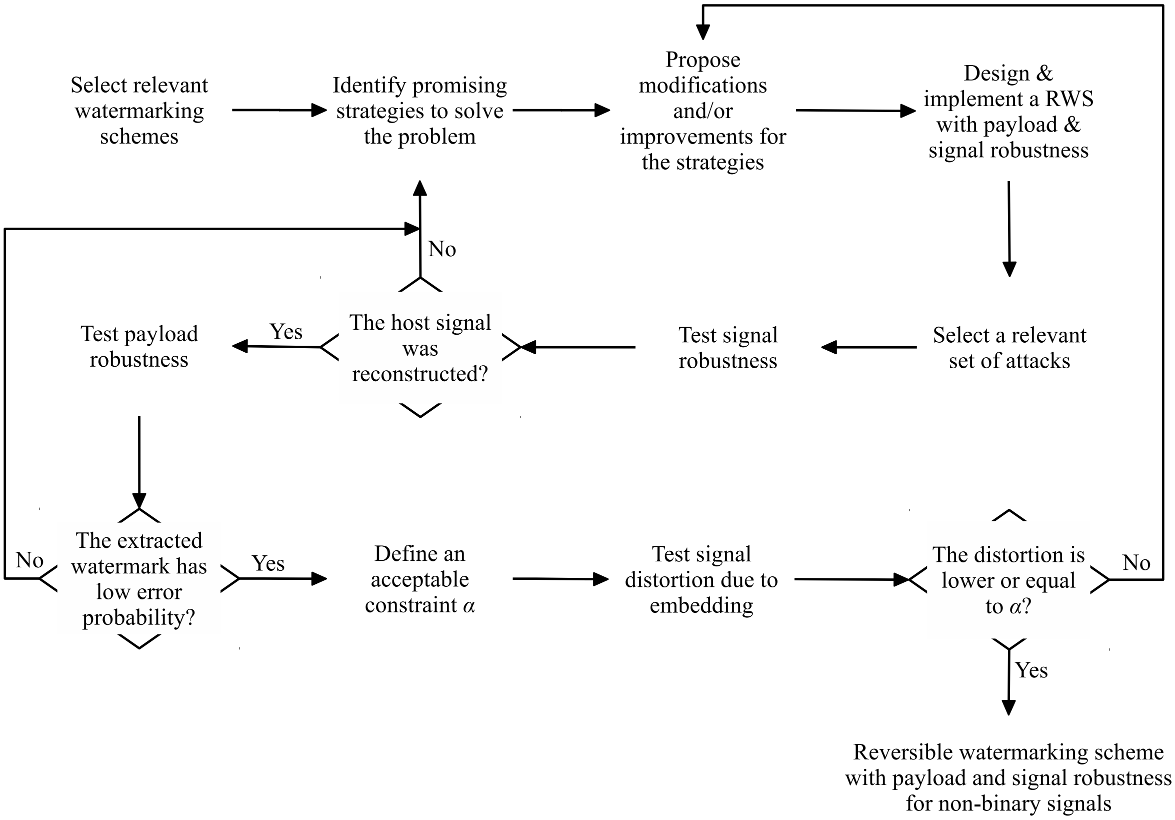

Select relevant watermarking schemes
Identify promising strategies to solve the problem
Propose modifications and/or improvements for the strategies
Design & implement a RWS with payload & signal robustness
No
Test payload robustness
Yes
The host signal was reconstructed?
Test signal robustness
Select a relevant set of attacks
No
The extracted watermark has low error probability?
Yes
Define an acceptable constraint α
Test signal distortion due to embedding
The distortion is lower or equal to α?
No
Yes
Reversible watermarking scheme with payload and signal robustness for non-binary signals

Fig. 4.3: Steps in the proposed methodology.

A brief description of the steps in this methodology will now be given:

1. **Select relevant watermarking schemes.** In this step existing work in the literature, related to the problem stated in this proposal will be selected and studied, in order to understand their underlying concepts and how those concepts can be used to solve the stated problem.
2. **Identify promising strategies to solve the problem.** Given the existing watermarking schemes selected before, some strategies will be developed, taking into consideration how the fundamental concepts of the schemes attack the problem and how they can be exploited to modify them or extend them to achieve the objectives of this proposal.
3. **Propose modifications and/or improvements for the strategies.** Once the possible strategies are stated, modifications and/or improvements to those concepts will be designed. In this step, new strategies will be proposed and/or improvements will be made to the existing works. Schemes not so closely related to the problem of focus might be used to complement the strategies or to propose new ones.
4. **Design and implement a reversible watermarking scheme (RWS) with payload and signal robustness.** Here the strategies previously identified will be combined or included to some existing methods, in order to construct a new reversible watermarking scheme with payload and signal robustness for non-binary audio signals. This new scheme can be of “type 1”, “type 2” or some other type that might be proposed later and will be implemented for incoming experiments.
5. **Select a relevant set of attacks.** Depending on the type of signal that was considered in the design of the watermarking scheme previously implemented, the set of attacks will be selected.

The first versions of the scheme will be designed for images, so a set of attacks for images will be constructed and later on equivalent or similar attacks for audio will be selected.

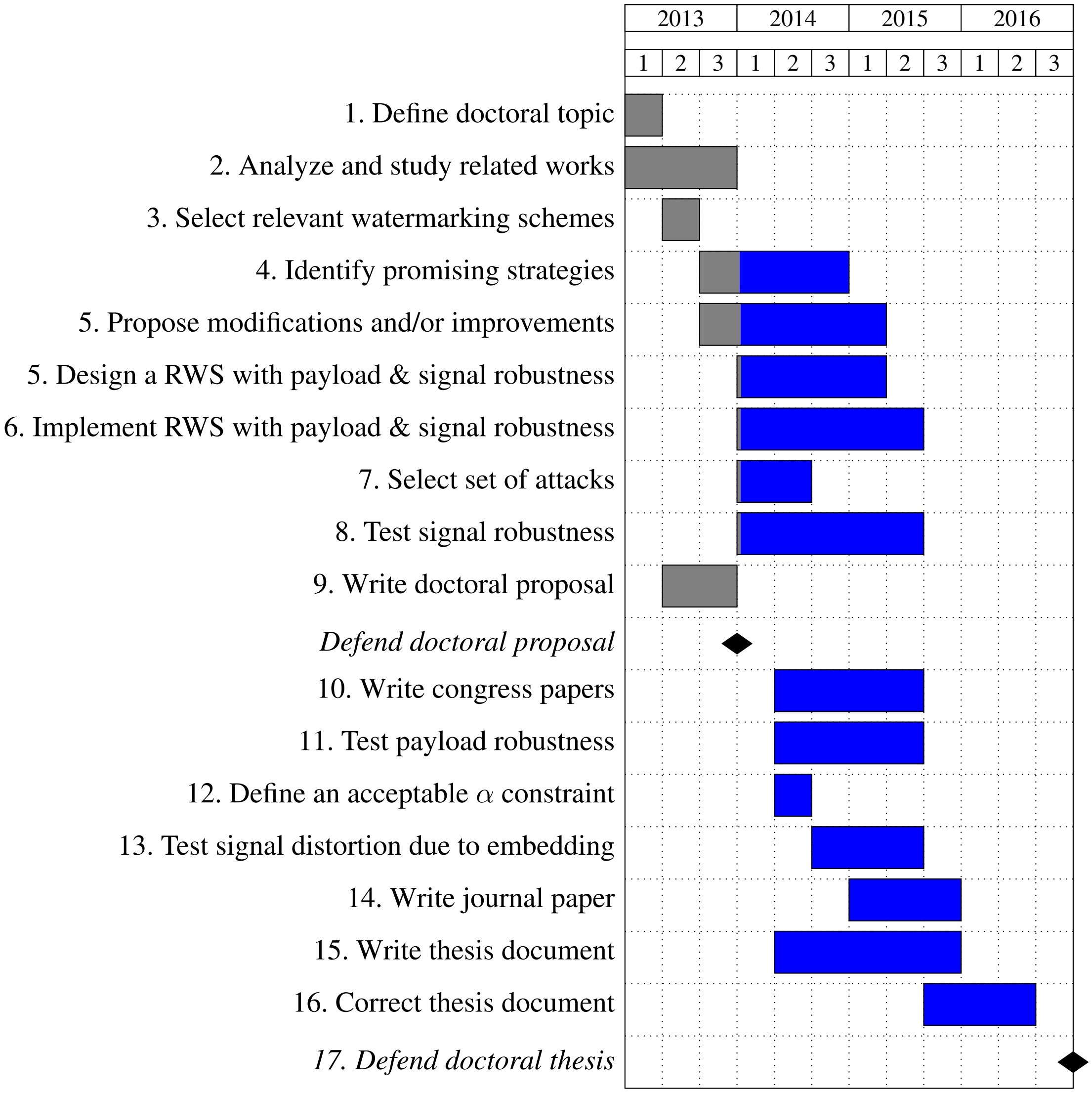
6. **Test signal robustness.** The first experiments will be design with the objective of testing the robustness of the audio signal against the attacks previously selected. Given that the proposed scheme should be a reversible one, the audio that is reconstructed with the extraction/restoration process must be exactly as the host audio, *i. e.*, the values of their samples must be exactly the same. The difference between those signals can be measured with the PSNR for images or SNR for audio signals. If the proposed scheme does not achieve a perfect reconstruction of the signal, then another strategy will be implemented and tested. Otherwise, the currently proposed scheme will be tested for payload robustness.
7. **Test payload robustness.** This set of experiments will be designed in order to test the robustness of the payload against the attacks. In this case, the extraction/restoration process of the proposed scheme will extract the embedded watermark that will be compared against the original watermark. The differences between the original and extracted watermark will be measured with the bit error rate (BER). If the values of BER for the experiments are over an error constraint, then another strategy will be implemented and tested. Otherwise, the final set of experiments to test the proposed scheme will be performed.
8. **Define an acceptable constraint α.** The distortion due to embedding constraint α will depend, again, on the type of signal that was considered during the design of the proposed scheme. This constraint will also depend on the possible applications.
9. **Test signal distortion due to embedding.** In this final set of experiments the signal marked with the proposed scheme will be compared against the host signal using the PSNR or SNR, depending on the signal. If this distortion between signals is higher than the constraint α, then the scheme will be modified; otherwise, the proposed scheme will be a solution to the problem.

When the proposed reversible watermarking scheme with payload and signal robustness for images fulfills the characteristics that are required, modifications to the scheme must be done again in order to translate it to a reversible watermarking scheme for audio signals, so the methodology will be followed again starting from step 3, in step 5 a set of audio attacks instead of image attacks will be selected and in step 8 the α constraint will be redefined in order to agree with applications for audio signals.

4.5 Expected contributions

- A mechanism that can select relevant characteristics of an audio signal in order to construct control data that has the property of being robust against a set of attacks. The size of this control data must be small enough to fit into an audio signal without causing noticeable distortions, but big enough to contain the neccesary information in order to reconstruct the original audio signal.
- An embedding process that inserts a watermark and the relevant characteristics selected before into a host audio signal, meeting an α constraint.
- A watermark extraction mechanism that recovers a watermark and control data hidden in an attacked audio signal, the extracted message has a low error probability.
- A signal restoration mechanism that can reconstruct a host audio signal, given an audio signal with distortion due to attacks β, distortion due to embedding α and control data that has relevant characteristics of the host audio signal.

4.6 Work plan



5 Preliminary results

As mentioned in the previous section, the line considered as the starting point in this research takes a reversible watermarking scheme with signal robustness as the base to make modifications and/or improvements, designed to make possible the insertion of useful payload along with the control data already embedded. Two strategies have been established that follow this idea, referred as "type 1" and "type 2" schemes (see 4.4). The first approach is the design of a type 1 scheme, based on a fragile reversible watermarking scheme and a reversible watermarking scheme with signal robustness.

5.1 Approach on a "type 1" scheme

In order to construct a type 1 scheme (see Figure 4.2) two existing reversible schemes were selected:

- the fragile reversible watermarking scheme by Sachnev *et al.* [SKSS10] and,
- the reversible watermarking scheme with signal robustness by Zhang *et al.* [ZW08].

The embedding and restoration procedures from these two schemes were concatenated according to Figure 4.2. First a watermarked image (Y) is created with Sachnev's scheme, then that watermarked image is robustly protected (Y') with Zhang's scheme. After attacks, the extraction/restoration process restores the watermarked image (Y') applying Zhang's scheme and finally, the host image (X) is reconstructed and the secret message (M') is recovered with Sachnev's scheme.

5.2 Experiments and results

The idea behind this first approach is to determine whether it is possible to insert a useful payload in a carrier image, where both the payload and the image can be reconstructed even in the presence of attacks. In order to evaluate this, three steps must be followed:

1. **Embedding.** Insert a watermark M into a host image X, producing a watermarked image Y and then protecting Y by embedding control data into itself, producing a protected watermarked image Y'. These operations impose a degradation over each version of the image (watermarked and protected) that must be measured in order to know the degradation caused bythe embedding procedure.
2. **Attacks.** Modify some pixels of the protected watermarked image Y to produce an attacked version $\hat{Y}$. The differences between $\hat{Y}$ and Y are measured in order to determine the degradation that the attack produced.
3. **Restoration and extraction.** Given an attacked image $\hat{Y}$, reconstruct the watermarked image Y, from which the host image X will be reconstructed and a watermark M' will be extracted. Given the fact that this scheme should have both payload and signal robustness, not only the image X must be perfectly reconstructed but the extracted watermark M' should also be equal to the inserted watermark M.

The degradation between a modified image against a reference one is measured with the PSNR, given by the formula:

$$\text{PSNR} = 20log_{10}\frac{255}{\sqrt{\text{MSE}}} \tag{4}$$

where MSE is the Mean Square Error, given by:

$$\text{MSE} = \frac{\sum_m^M \sum_n^N (X_{m,n} - Y_{m,n})^2}{M \times N} \tag{5}$$

where $X_{m,n}$ is the pixel at the m^{th} row and n^{th} column of the host image, $Y_{m,n}$ is the pixel at the m^{th} row and n^{th} column of the modified image, M is the number of rows and N is the number of columns in the images. In order to compare the differences between an embedded watermark against a recovered one, the Bit Error Rate (BER) is used, given with the formula:

$$\text{BER} = \frac{\text{Errors}}{N_{bits}} \tag{6}$$

where N_{bits} is the total number of bits and Errors is given by:

$$\text{Errors} = \sum_{n}^{N} \begin{cases} 1, W'_n \neq W_n \\ 0, W'_n = W_n \end{cases} \tag{7}$$

Embedding.

These experiments insert a binary image of 210×210 as a secret message into a grayscale test host image of 512×512 and three PSNR values are collected. A PSNR$_{\text{WM}}$ value is measured between the host image (X) and the watermarked image (Y); a PSNR$_{\text{PR}}$ value is measured between the watermarked image (Y) and the protected watermarked version (Y'); and a PSNR$_{\text{F}}$ value is calculated between the host image (X) and the protected watermarked one (Y'). The results of embedding the binary image 5.1 into 9 test images are listed in Table 6.

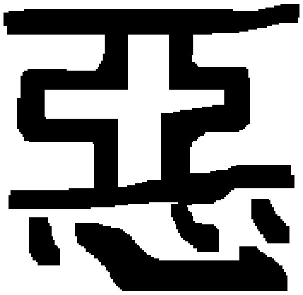
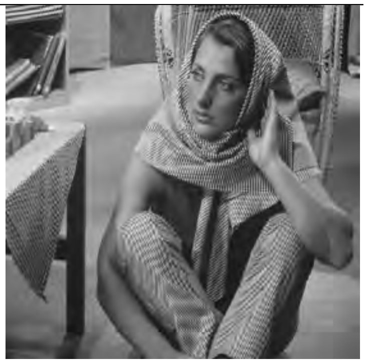


Fig. 5.1: Binary image inserted as a watermark.

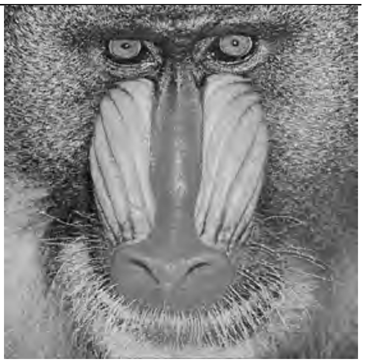
Table 6: Measured PSNR in dB after watermark embedding.

Host image	PSNR$_{\text{WM}}$	PSNR$_{\text{PR}}$	PSNR$_{\text{F}}$	Protected image
	41.2324	23.6029	23.3194	

Continues on next page

Host image	**PSNR$_{WM}$**	**PSNR$_{PR}$**	**PSNR$_{F}$**	**Protected image**
	43.5492	27.2920	26.9928	
	43.2524	27.8966	27.5334	
	40.9796	25.0173	24.5605	
	42.2199	28.9784	28.3729	

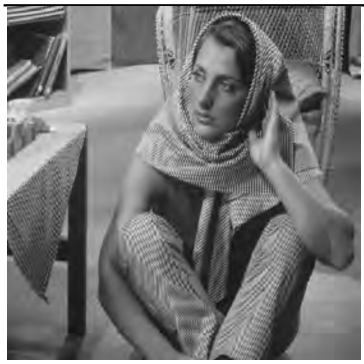
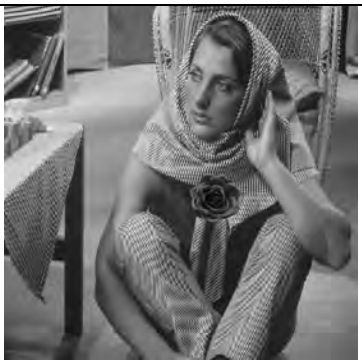
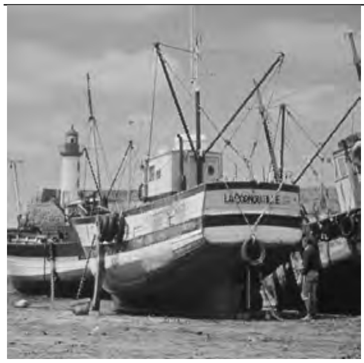
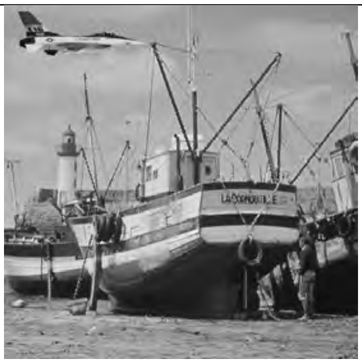
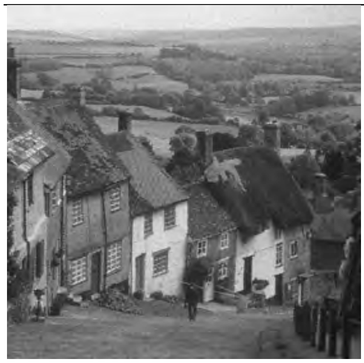
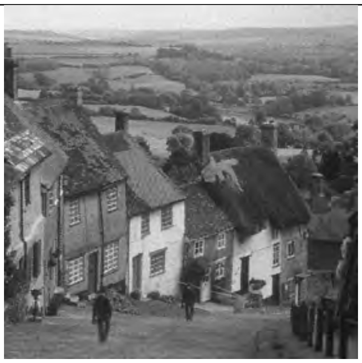
Continues on next page

Host image	**PSNR$_{\mathrm{WM}}$**	**PSNR$_{\mathrm{PR}}$**	**PSNR$_{\mathrm{F}}$**	**Protected image**
	36.7589	20.7862	20.1497	
	41.7419	28.4460	27.7728	
	41.8436	31.2718	30.1858	
	42.3845	31.8814	30.8149	
Average	41.5513	27.2414	26.6335	

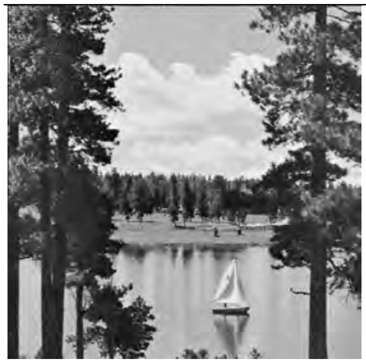
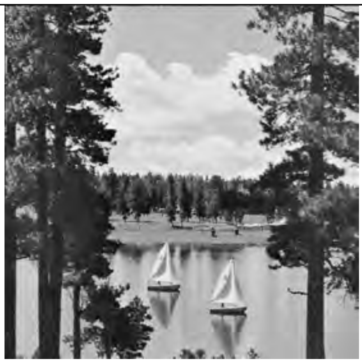
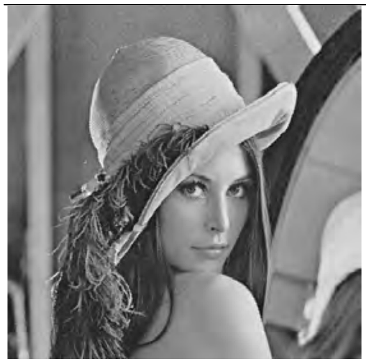
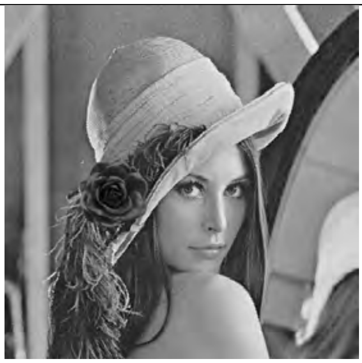
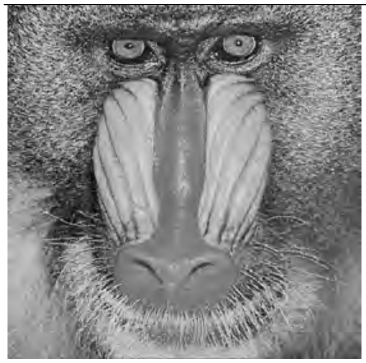
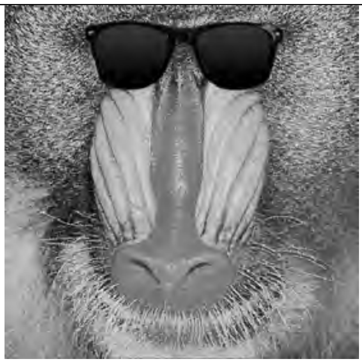
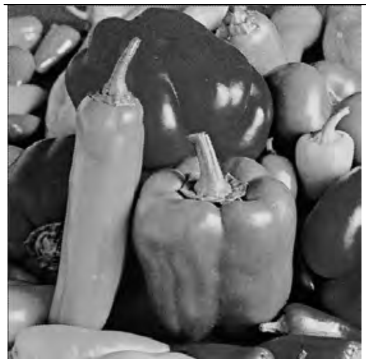
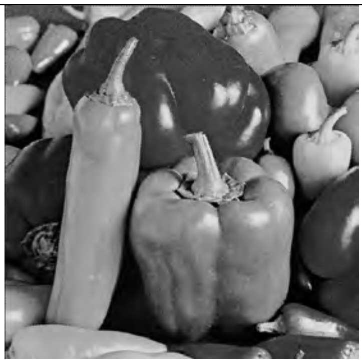
Attacks.

To test the robustness of the proposed scheme, the protected watermarked images were subjected to a content replacement attack, where some pixels of the image were changed by a region of pixels from another image. The distortions caused by this attack were measured in terms of PSNR values and the results for the 9 test images are presented in Table 7.

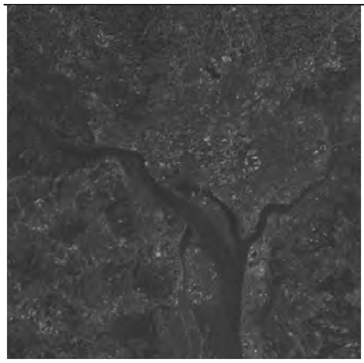
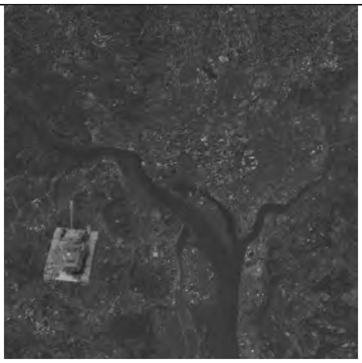
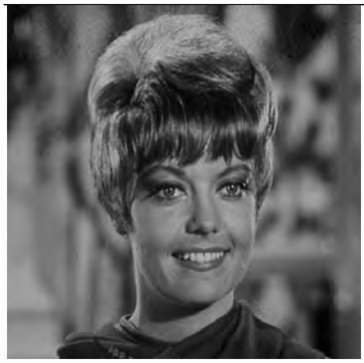
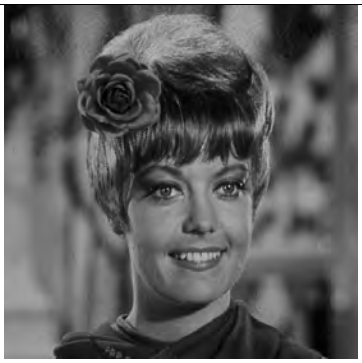
Table 7: Measured PSNR in dB after content replacement attack.

Protected image	Attacked image	PSNR
		22.6025
		24.6378
		26.9119

Continues on next page

Protected image	Attacked image	PSNR
		23.5747
		25.6881
		17.5189
		25.6630

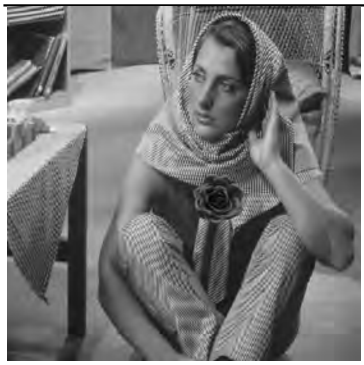
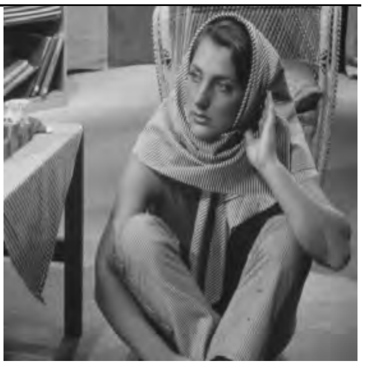
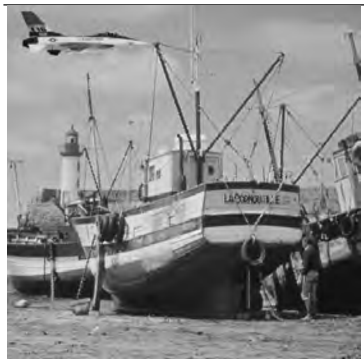
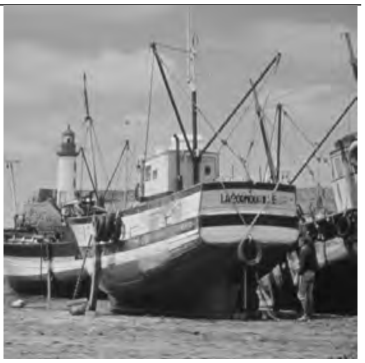
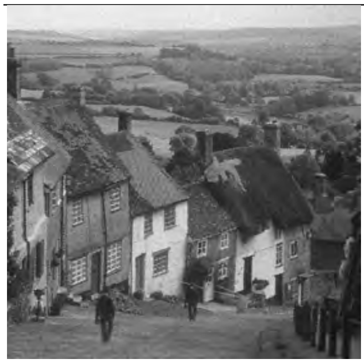
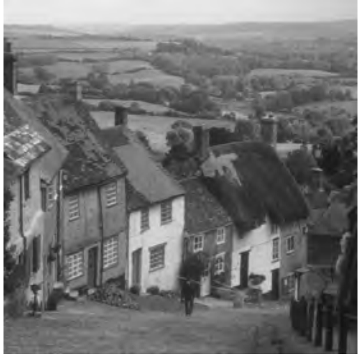
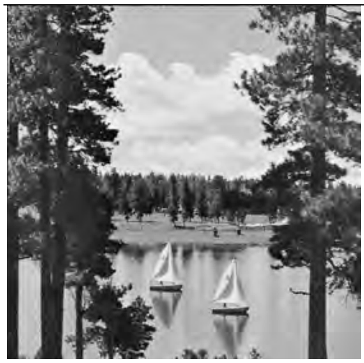
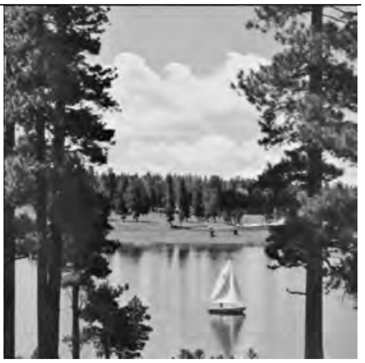
Continues on next page

Protected image	**Attacked image**	**PSNR**
		27.9454
		25.0513

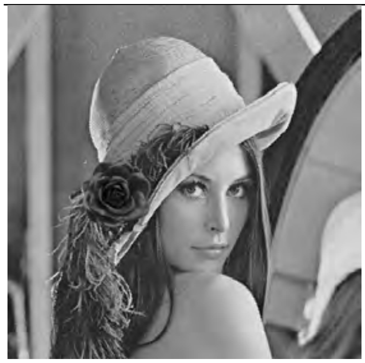
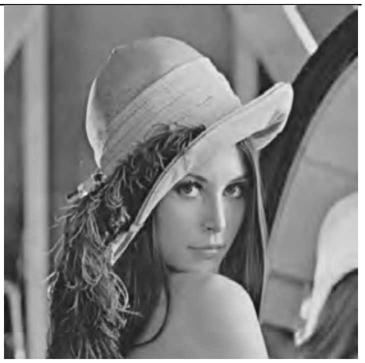
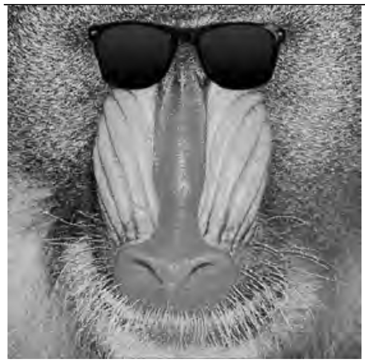
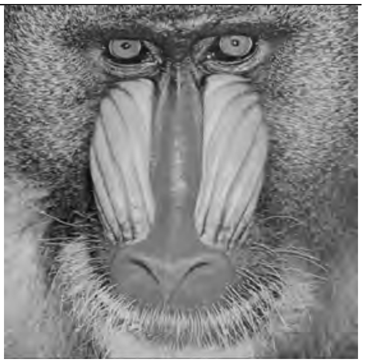
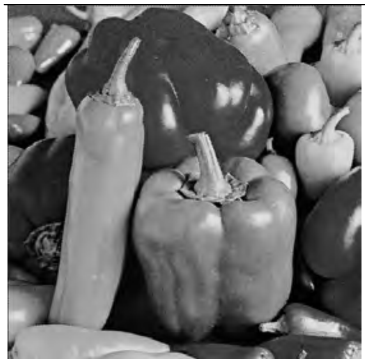
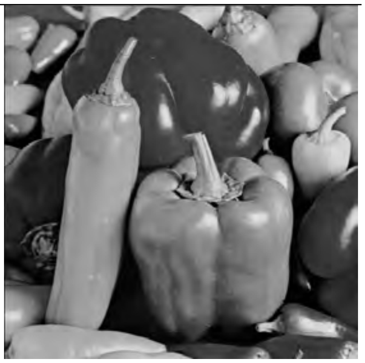
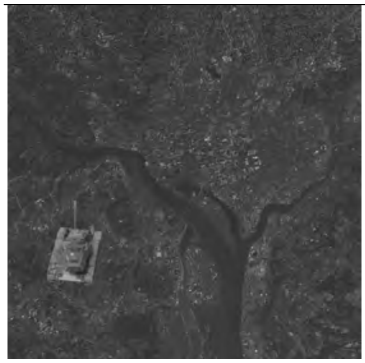
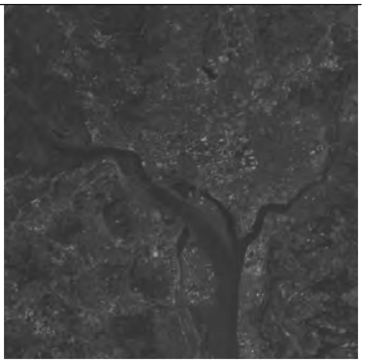
Restoration and extraction.

The objective of these experiments is to validate the robustness of the embedded watermark and the reconstructed image against the content replacement attack. These experiments take an attacked image ($\hat{Y}$) and reconstruct the watermarked version (Y), then the host signal (X) is reconstructed and a watermark is extracted (M'), both from the watermarked signal just reconstructed (Y); two PSNR values from these steps are collected and the BER between the embedded and extracted watermarks is calculated. A PSNR_{RWM} value is measured between the reconstructed watermarked image (Y) and the host image (X); this PSNR_{RWM} must be the same as the PSNR_{WM} from the embedding process. A PSNR_{RF} value is measured between the final reconstructed image and the host one. The collected PSNR values for the 9 test images are presented in Table 8 and the calculated BER values for the watermark extracted from the 9 test images are given in Table 9.

Table 8: Measured PSNR in dB after restoration.

Attacked image	**PSNR$_{\text{RWM}}$**	**PSNR$_{\text{RF}}$**	**Restored image**
	41.2324	∞	
	43.5492	∞	
	43.2524	∞	
	40.9796	∞	

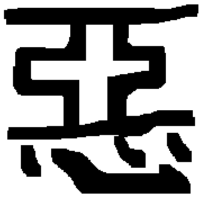
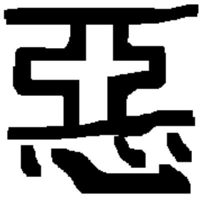
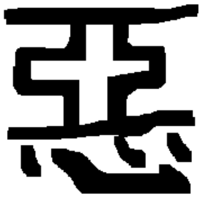
Continues on next page

Attacked image	PSNR$_{RWM}$	PSNR$_{RF}$	Restored image
	42.2199	∞	
	36.7589	∞	
	41.7419	∞	
	41.8436	∞	

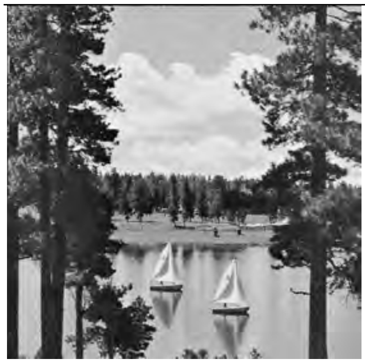
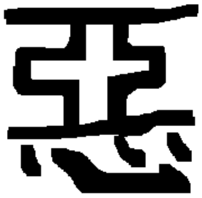
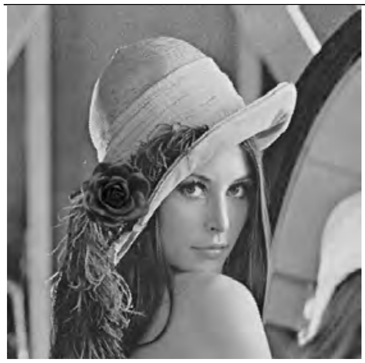
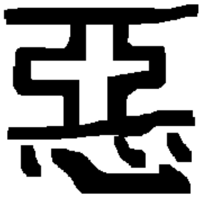
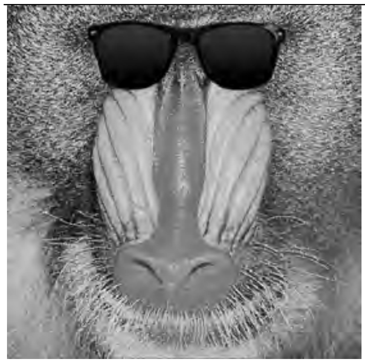
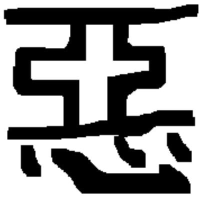
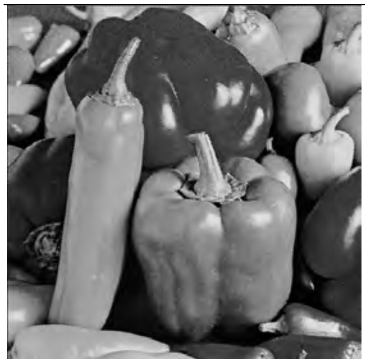
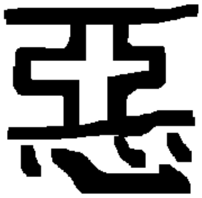
Continues on next page

Attacked image	$\mathrm{PSNR}_{\mathrm{RWM}}$	$\mathrm{PSNR}_{\mathrm{RF}}$	Restored image
	42.3845	∞	

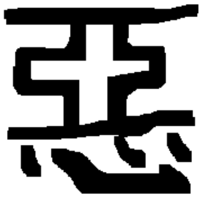
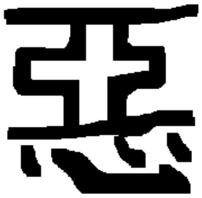
Table 9: BER for the extracted watermark.

Attacked image	Extracted watermark	BER
		0.0000
		0.0000
		0.0000

Continues on next page

Attacked image	Extracted watermark	BER
		0.0000
		0.0000
		0.0000
		0.0000

Continues on next page

Attacked image	Extracted watermark	BER
		0.0000
		0.0000

From Table 6 it can be seen that the embedding process has an average distortion of 26.63 dB, which is lower than the 40 dB value recommended for most watermarking schemes. However, the scheme could be used in applications with a higher tolerance for distortions. The PSNR_{WM} values in that same table are equal to those of PSNR_{RWM} in Table 8, which means that the watermarked image Y is perfectly reconstructed even after a content replacement attack. The PSNR_{RF} values of ∞ mean that the restored images have exactly the same values as the host ones. From Table 9 it can be seen that there are no errors in the extracted watermarked images.

These results indicate that the proposed scheme has payload and signal robustness against content replacement attack, although under the same circumstances as in the scheme proposed by Zhang *et al.* [ZW08]. The drawbacks of both schemes are that the tampering cannot be corrected if the tampered area is greater than 3.2% of the image, because the reconstruction of the missing pixels depends on finding the solution of a binary linear equation system. In case of a modification greater than 3.2% of the image, the restoration process cannot reconstruct a watermarked signal Y and therefore, the extraction process does not reconstruct the host image neither extracts the hidden watermark M'.

Although this research focuses on the design of a reversible watermarking scheme with payload and signal robustness for audio signals, the experiments were designed for images because that is the type of media that the reference schemes utilice. A reversible watermarking schemes with the characteristics described so far will first be designed for image signals and later those underlying strategies will be adapted for the characteristics of audio signals.

At first the convertion of the scheme from image to audio signals might seem as a trivial task. However, it implicates more than just a convertion from a two-dimensional to a one-dimensional space. Just the design of a mechanism that selects relevant characteristics for audio signals instead of image signals is a challenging work.

6 Conclusions

The design of a reversible watermarking scheme that extracts a watermark with low error probability and reconstructs a host signal from a watermarked signal that was subjected to attacks is not a trivial task. A reversible watermarking scheme with these characteristics has to foresee the possible modifications that a set of attacks may create into the watermarked signal. Those modifications might be extensive and could damage different aspects of an audio signal, depending on the type and number of attacks considered to be in this set.

This kind of scheme should then construct control data to protect the watermarked signal from the attacks and it should be embedded along with a payload. However, there is the restriction that the insertion of the control data and the watermark should not alter the signal in a noticeable way. Therefore, a reversible watermarking scheme with payload and signal robustness must make a trade-off between the robustness and the size of the control data.

This research proposal seeks the design of a reversible watermarking scheme that is capable of reconstructing a host signal and extract a hidden watermark after the watermarked signal is submitted to attacks. This scheme should take into consideration that the constructed control data should be small enough to keep a low distortion after embedding, but it should contain enough information to be able to reconstruct the original signal and at the same time it must be robust enough to survive the modifications caused by the attacks.

The preliminary results demonstrate that it is possible to design a reversible watermarking scheme with payload and signal robustness; although the robustness and the embedding distortion of the proposed scheme can be improved. But these results suggest that it is possible to design a solution for the stated problem with the characteristics previously mentioned.

The proposed scheme must be modified to reduce the perceptual distortion caused by the embedding process and it has to be tested for a wider range of attacks, in order to determine its robustness. The scheme could also be modified to reach robustness for other attacks along with the current one. Later, the scheme must be translated to work with audio signals considering attacks for audio similar or equivalent to the attacks considered for images. It must also be taken into consideration that the characteristics for image signals are different from the characteristics for audio ones, so the strategies employed for images might not be directly used for audio signals.

From the analysis of the related work, it can be seen that the problem stated in this research is important because there are applications where it is necessary to be able to reconstruct an unmodified audio along with its secret information, regardless of attacks and to date there are no schemes that satisfy these characteristics. The preliminary results show that it is possible to design such a scheme under the considered time and following the proposed methodology.

References

AGL$^+$12. Lingling An, Xinbo Gao, Xuelong Li, Dacheng Tao, Cheng Deng, and Jie Li. Robust reversible watermarking via clustering and enhanced pixel-wise masking. *IEEE Transactions on Image Processing*, 21(8):3598–3611, 2012.

AGY$^+$12. Lingling An, Xinbo Gao, Yuan Yuan, Dacheng Tao, Cheng Deng, and Feng Ji. Content-adaptive reliable robust lossless data embedding. *Neurocomputing*, 79(0):1–11, 2012.

AGYT12. Lingling An, Xinbo Gao, Yuan Yuan, and Dacheng Tao. Robust lossless data hiding using clustering and statistical quantity histogram. *Neurocomputing*, 77(1):1–11, 2012.

AMAC12. T. Ahsan, T. Mohammad, M.S. Alam, and Ui-Pil Chong. Digital watermarking based image authentication and restoration by quantization of integer wavelet transform coefficients. In *International Conference on Informatics, Electronics Vision (ICIEV), 2012*, pages 1163–1167, 2012.

BdB03. Marinus M. Boone and Werner P. J. de Bruijn. Improving Speech Intelligibility in Teleconferencing by using Wave Field Synthesis. In *Audio Engineering Society Convention 114*, Mar 2003.

Beg06. *Spatially Modulated Auditory Alerts for Aviation*, volume 54, 2006.

BSLN12a. S. Bravo-Solorio, C.-T. Li, and A.K. Nandi. Watermarking method with exact self-propagating restoration capabilities. In *IEEE International Workshop on Information Forensics and Security (WIFS), 2012*, pages 217–222, 2012.

BSLN12b. S. Bravo-Solorio, C.-T. Li, and A.K. Nandi. Watermarking with lowembedding distortion and self-propagating restoration capabilities. In *19th IEEE International Conference on Image Processing (ICIP), 2012*, pages 2197–2200, 2012.

CBC$^+$03. Roberto Caldelli, Franco Bartolini, Vito Cappellini, Alessandro Piva, and Mauro Barni. A New Self-Recovery Technique for Image Authentication. In Narciso Garcia, Luis Salgado, and Jose M. Martinez, editors, *Visual Content Processing and Representation*, volume 2849 of *Lecture Notes in Computer Science*, pages 164–171. Springer Berlin Heidelberg, 2003.

CC07. D. Coltuc and J.-M. Chassery. Very Fast Watermarking by Reversible Contrast Mapping. *IEEE Signal Processing Letters*, 14(4):255–258, 2007.

CCCK09. Abbas Cheddad, Joan Condell, Kevin Curran, and Paul Mc Kevitt. A secure and improved self-embedding algorithm to combat digital document forgery. *Signal Processing*, 89(12):2324–2332, 2009.

CFNS06. Michael Cohen, Owen Noel Newton Fernando, Tatsuya Nagai, and Kensuke Shimizu. "Back-Seat Driver": Spatial Sound for Vehicular Way-Finding and Situation Awareness. In *Proceedings of the Japan-China Joint Workshop on Frontier of Computer Science and Technology*, FCST '06, pages 109–115, Washington, DC, USA, 2006. IEEE Computer Society.

CFSX07. E Chrysochos, V Fotopoulos, AN Skodras, and M Xenos. Reversible image watermarking based on histogram modification. In *11th Panhellenic Conference on Informatics (PCI 2007)*, pages 93–104, 2007.

CHW08. Fan Chen, Hongjie He, and Hongxia Wang. A Fragile Watermarking Scheme for Audio Detection and Recovery. In *Congress on Image and Signal Processing, 2008. CISP '08.*, volume 5, pages 135–138, 2008.

CLY09. Chin-Chen Chang, Pei-Yu Lin, and Jieh-Shan Yeh. Preserving robustness and removability for digital watermarks using subsampling and difference correlation. *Information Sciences*, 179(13):2283–2293, 2009.

CMB$^+$08. I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker. *Digital Watermarking and Steganography*. The Morgan Kaufmann Series in Multimedia Information and Systems. Elsevier Science, 2008.

CMHR07. G. Coatrieux, J. Montagner, H. Huang, and C. Roux. Mixed Reversible and RONI Watermarking for Medical Image Reliability Protection. In *29th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, 2007. EMBS 2007*, pages 5653–5656, 2007.

CRMH10. Clara Cruz, Reyes Rogelio, Nakano Mariko, and Perez Hector. Semi-fragile watermarking based content image authentication scheme. *Revista Facultad de Ingeniería Universidad de Antioquia*, pages 160–169, 12 2010.

CS08. Nedeljko Cvejic and Tapio Seppänen. *Digital Audio Watermarking Techniques and Technologies*. Information Science Reference, 2008.

CSTS02. Mehmet U Celik, Gaurav Sharma, A Murat Tekalp, and Eli S Saber. Video authentication with self-recovery. In *Electronic Imaging 2002*, pages 531–541. International Society for Optics and Photonics, 2002.

DDM03. C. De Vleeschouwer, J.-F. Delaigle, and B. Macq. Circular interpretation of bijective transformations in lossless watermarking for media asset management. *Multimedia, IEEE Transactions on*, 5(1):97–105, 2003.

FG99a. J. Fridrich and M. Goljan. Images with self-correcting capabilities. In *International Conference on Image Processing, 1999. ICIP 99.*, volume 3, pages 792–796, 1999.

FG99b. Jiri Fridrich and Miroslav Goljan. Protection of digital images using self embedding. In *Symposium on Content Security and Data Hiding in Digital Media*. Newark, NJ, USA, 1999.

FGD02. Jessica Fridrich, Miroslav Goljan, and Rui Du. Lossless Data Embedding – New Paradigm in Digital Watermarking. *EURASIP Journal on Applied Signal Processing*, 2002(2):185–196, February 2002.

GAY$^+$11. Xinbo Gao, Lingling An, Yuan Yuan, Dacheng Tao, and Xuelong Li. Lossless Data Embedding Using Generalized Statistical Quantity Histogram. *IEEE Transactions on Circuits and Systems for Video Technology*, 21(8):1061–1070, 2011.

GCG$^+$02. Emilia Gómez, P. Cano, L. Gomes, E. Batlle, and M. Bonnet. Mixed Watermarking-Fingerprinting Approach for Integrity Verification of Audio Recordings. 2002.

GG07. Tie-Gang Gao and Qiao-Lun Gu. Reversible watermarking algorithm based on wavelet lifting scheme. In *International Conference on Wavelet Analysis and Pattern Recognition, 2007. ICWAPR '07*, volume 4, pages 1771–1775, 2007.

GHGC09. QiaoLun Gu, Guanglin Han, Tiegang Gao, and Zengqiang Chen. A Novel Adaptive Reversible Watermarking Algorithm Based on Wavelet Lifting Scheme. In *International Conference on Information Engineering and Computer Science, 2009. ICIECS 2009*, pages 1–4, 2009.

HAHH$^+$09. Ammar M. Hassan, Ayoub Al-Hamadi, Yassin M. Y. Hasan, Mohamed A. A. Wahab, and Bernd Michaelis. Secure Block-Based Video Authentication with Localization and Self-Recovery. *World Academy of Science, Engineering and Technology*, 2009(33):69–74, September 2009.

HAHH$^+$10. A. M. Hassan, A. Al-Hamadi, Y. M Y Hasan, M. A A Wahab, A. Panning, and B. Michaelis. Variable block-size image authentication with localization and self-recovery. In *17th IEEE International Conference on Image Processing (ICIP), 2010*, pages 3665–3668, 2010.

HAHM$^+$10. A.M. Hassan, A. Al-Hamadi, B. Michaelis, Y. M Y Hasan, and M. A A Wahab. Secure Self-Recovery Image Authentication Using Randomly-Sized Blocks. In *20th International Conference on Pattern Recognition (ICPR), 2010*, pages 1445–1448, 2010.

HC07. KuoLung Hung and Chin-Chen Chang. Recoverable Tamper Proofing Technique for Image Authentication Using Irregular Sampling Coding. In Bin Xiao, LaurenceT. Yang, Jianhua Ma, Christian Muller-Schloer, and Yu Hua, editors, *Autonomic and Trusted Computing*, volume 4610 of *Lecture Notes in Computer Science*, pages 333–343. Springer Berlin Heidelberg, 2007.

HCT$^+$12. Hongjie He, Fan Chen, Heng-Ming Tai, T. Kalker, and Jiashu Zhang. Performance Analysis of a Block-Neighborhood-Based Self-Recovery Fragile Watermarking Scheme. *IEEE Transactions on Information Forensics and Security*, 7(1):185–196, 2012.

HH07. Y. M Y Hasan and A.M. Hassan. Tamper Detection with Self-Correction Hybrid Spatial-DCT Domains Image Authentication Technique. In *IEEE International Symposium on Signal Processing and Information Technology, 2007*, pages 369–374, 2007.

HR00. F. Hartung and F. Ramme. Digital rights management and watermarking of multimedia content for m-commerce applications. *Communications Magazine, IEEE*, 38(11):78–84, 2000.

HZC08. HongJie He, JiaShu Zhang, and Fan Chen. A self-recovery fragile watermarking scheme for image authentication with superior localization. *Science in China Series F: Information Sciences*, 51(10):1487–1507, 2008.

HZT09. Hong-Jie He, Jia-Shu Zhang, and Heng-Ming Tai. Self-recovery Fragile Watermarking Using Block-Neighborhood Tampering Characterization. In Stefan Katzenbeisser and Ahmad-Reza Sadeghi, editors, *Information Hiding*, volume 5806 of *Lecture Notes in Computer Science*, pages 132–145. Springer Berlin Heidelberg, 2009.

IHSO10. M. Iwata, T. Hori, A. Shiozaki, and A. Ogihara. Digital watermarking method for tamper detection and recovery of JPEG images. In *International Symposium on Information Theory and its Applications (ISITA), 2010*, pages 309–314, 2010.

JL08. Xuemei Jiang and Quan Liu. Semi-fragile watermarking algorithm for image tampers localization and recovery. *Journal of Electronics (China)*, 25(3):343–351, 2008.

KD12. P. Korus and A. Dziech. Reconfigurable self-embedding with high quality restoration under extensive tampering. In *19th IEEE International Conference on Image Processing (ICIP), 2012*, pages 2193–2196, 2012.

KD13. P. Korus and A. Dziech. Efficient Method for Content Reconstruction With Self-Embedding. *IEEE Transactions on Image Processing*, 22(3):1134–1147, 2013.

KE09. A Karantonis and J Ellinas. Self embedding watermarking for preventing image content from tampering. 2009.

KJR11. Pawel Korus, Lucjan Janowski, and Piotr Romaniak. Automatic quality control of digital image content reconstruction schemes. In *IEEE International Conference on Multimedia and Expo (ICME), 2011*, pages 1–6, 2011.

KL05. Shivaprasad Kotagiri and J Nicholas Laneman. Reversible information embedding in multi-user channels. In *Allerton Conference on Communications, Control, and Computing*. Citeseer, 2005.

KL06. Shivaprasad Kotagiri and J.N. Laneman. Information Embedding in Degraded Broadcast Channels. In *IEEE International Symposium on Information Theory, 2006*, pages 494–498, 2006.

KLSL09. Kyung-Su Kim, Min-Jeong Lee, Young-Ho Suh, and Heung-Kyu Lee. Robust lossless data hiding based on block gravity center for selective authentication. In *IEEE International Conference on Multimedia and Expo, 2009. ICME 2009*, pages 1022–1025, 2009.

KSD10. P. Korus, W. Szmuc, and A. Dziech. A scheme for censorship of sensitive image content with high-quality reconstruction ability. In *IEEE International Conference on Multimedia and Expo (ICME), 2010*, pages 1073–1078, 2010.

KW03. TON Kalker and Frans M Willems. Capacity bounds and constructions for reversible data-hiding. In *Security and Watermarking of Multimedia Contents V*, volume 5020, pages 604–611, 2003.

LHH05. Phen Lan Lin, Chung-Kai Hsieh, and Po-Whei Huang. A hierarchical digital watermarking method for image tamper detection and recovery. *Pattern Recognition*, 38(12):2519–2529, 2005.

Lu04. Chun-Shien Lu. *Multimedia Security: Steganography and Digital Watermarking Techniques for Protection of Intellectual Property*. IGI Publishing, Hershey, PA, USA, 2004.

LWMZ11. Chunlei Li, Yunhong Wang, Bin Ma, and Zhaoxiang Zhang. A novel self-recovery fragile watermarking scheme based on dual-redundant-ring structure. *Computers & Electrical Engineering*, 37(6):927–940, 2011.

ME01. Bijan G. Mobasseri and Aaron T. Evans. Content-dependent video authentication by self-watermarking in color space. In *SPIE Proceedings in Security and Watermarking of Multimedia Contents III*, volume 4314, pages 35–44. International Society of Optics and Photonics, August 2001.

MGL98. Loomis Jack M., Golledge Reginald G., and Klatzky Roberta L. Navigation System for the Blind: Auditory Display Modes and Guidance. *Presence: Teleoperators and Virtual Environments*, 7(2):193–203, 1998. doi: 10.1162/105474698565677.

MNKMM11. Jose Antonio Mendoza-Noriega, M Kurkoski, Mariko Nakano Miyatake, and Hector Perez Meana. Image authentication and recovery using BCH error-correcting codes. *International Journal of Computers*, 5(1):26–33, 2011.

MNKNMPM10. J.A. Mendoza-Noriega, B.M. Kurkoski, M. Nakano-Miyatake, and H. Perez-Meana. Halftoning-based self-embedding watermarking for image authentication and recovery. In *53rd IEEE International Midwest Symposium on Circuits and Systems (MWSCAS), 2010*, pages 612–615, 2010.

Mob00. B.G. Mobasseri. A spatial digital video watermark that survives MPEG. In *International Conference on Information Technology: Coding and Computing, 2000.*, pages 68–73, 2000.

NSA+04. Zhicheng Ni, Y.Q. Shi, N. Ansari, Wei Su, Q. Sun, and Xiao Lin. Robust lossless image data hiding. In *IEEE International Conference on Multimedia and Expo, 2004. ICME '04*, volume 3, pages 2199–2202, 2004.

NSA+08. Zhicheng Ni, Y.Q. Shi, N. Ansari, Wei Su, Q. Sun, and Xiao Lin. Robust lossless image data hiding designed for semi-fragile image authentication. *IEEE Transactions on Circuits and Systems for Video Technology*, 18(4):497–509, 2008.

PLR09. Tony Poitschke, Florian Laquai, and Gerhard Rigoll. Guiding a Driver's Visual Attention Using Graphical and Auditory Animations. In Don Harris, editor, *Engineering Psychology and Cognitive Ergonomics*, volume 5639 of *Lecture Notes in Computer Science*, pages 424–433. Springer Berlin Heidelberg, 2009.

QCC12. Chuan Qin, Chin-Chen Chang, and Pei-Yu Chen. Self-embedding fragile watermarking with restoration capability based on adaptive bit allocation mechanism. *Signal Processing*, 92(4):1137–1150, 2012.

QF10. Zhenxing Qian and Guorui Feng. Inpainting Assisted Self Recovery With Decreased Embedding Data. *IEEE Signal Processing Letters*, 17(11):929–932, 2010.

QQ10. Zhenxing Qian and Tong Qiao. Image Self-Embedding with Large-Area Restoration Capability. In *International Conference on Multimedia Information Networking and Security (MINES), 2010*, pages 649–652, 2010.

SAM08. M.J. Saberian, M.A. Akhaee, and F. Marvasti. An invertible quantization based watermarking approach. In *IEEE International Conference on Acoustics, Speech and Signal Processing, 2008. ICASSP 2008*, pages 1677–1680, 2008.

SD03. Martin Steinebach and Jana Dittmann. Watermarking-based digital audio data authentication. *EURASIP Journal on Advances in Signal Processing*, 2003:1001–1015, January 2003.

Sei05. Juergen Seitz. *Digital Watermarking for Digital Media*. Information Science Publishing, 2005.

SKSS10. Vasiliy Sachnev, HyoungJoong Kim, Sundaram Suresh, and YunQing Shi. Reversible Watermarking Algorithm with Distortion Compensation. *EURASIP Journal on Advances in Signal Processing*, 2010(1):316820, 2010.

SQL+11. Yanjiao Shi, Miao Qi, Yinghua Lu, Jun Kong, and Danying Li. Object based self-embedding watermarking for video authentication. In *International Conference on Transportation, Mechanical, and Electrical Engineering (TMEE)*, pages 519–522, 2011.

SQY$^+$13. Yanjiao Shi, Miao Qi, Yugen Yi, Ming Zhang, and Jun Kong. Object based dual watermarking for video authentication. *Optik - International Journal for Light and Electron Optics*, 124(19):3827–3834, 2013.

SS09. O. Sumszyk and Y. Steinberg. Information embedding with reversible stegotext. In *IEEE International Symposium on Information Theory, 2009*, pages 2728–2732, 2009.

Ste06. Y. Steinberg. Reversible Information Embedding with Compressed Host at the Decoder. In *IEEE International Symposium on Information Theory, 2006* , pages 188–191, 2006.

Ste08a. Y. Steinberg. Coding for Channels With Rate-Limited Side Information at the Decoder, With Applications. *IEEE Transactions on Information Theory*, 54(9):4283–4295, 2008.

Ste08b. Y. Steinberg. Simultaneous transmission of data and state with common knowledge. In *IEEE International Symposium on Information Theory, 2008*, pages 935–939, 2008.

Ste09. Y. Steinberg. Coding and Common Reconstruction. *IEEE Transactions on Information Theory*, 55(11):4995–5010, 2009.

THR13. Deborah Theodoros, Anne Hill, and Trevor Russell. Advances int telehealth for the delivery of voice therapy: the australian experience. In *10th International Conference Advances in Quantitative Laryngology*, volume 8, page 15, 2013.

TTL10. H.-H. Tsai, H.-C. Tseng, and Y.-S. Lai. Robust lossless image watermarking based on α-trimmed mean algorithm and support vector machine. *Journal of Systems and Software*, 83(6):1015–1028, 2010. Software Architecture and Mobility.

WC02. Hsien-Chu Wu and Chin-Chen Chang. Detection and restoration of tampered JPEG compressed images. *Journal of Systems and Software*, 64(2):151–161, 2002.

WC07. Ming-Shi Wang and Wei-Che Chen. A majority-voting based watermarking scheme for color image tamper detection and recovery. *Computer Standards & Interfaces*, 29(5):561–570, 2007.

WK04. Frans MJ Willems and Ton Kalker. Coding theorems for reversible embedding. *DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, 66:61–78, 2004.

WT08. Shuenn-Shyang Wang and Sung-Lin Tsai. Automatic image authentication and recovery using fractal code embedding and image inpainting. *Pattern Recognition*, 41(2):701–712, 2008.

Wu07. Xiaoyun Wu. Reversible Semi-fragile Watermarking Based on Histogram Shifting of Integer Wavelet Coefficients. In *Inaugural IEEE International Conference on Digital Ecosystems and Technologies, 2007. IEEE DEST '07*, pages 501–505, 2007.

YLH10. Ching-Yu Yang, Chih-Hung Lin, and Wu-Chih Hu. Reversible Watermarking by Coefficient Adjustment Method. In *2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP)*, pages 39–42, 2010.

ZCY11. Weiming Zhang, Biao Chen, and Nenghai Yu. Capacity-Approaching Codes for Reversible Data Hiding. In Tomáš Filler, Tomáš Pevný, Scott Craver, and Andrew Ker, editors, *Information Hiding*, volume 6958 of *Lecture Notes in Computer Science*, pages 255–269. Springer Berlin Heidelberg, 2011.

ZCY12. Weiming Zhang, Biao Chen, and Nenghai Yu. Improving Various Reversible Data Hiding Schemes Via Optimal Codes for Binary Covers. *IEEE Transactions on Image Processing*, 21(6):2991–3003, 2012.

ZHLY13. Weiming Zhang, Xiaocheng Hu, Xiaolong Li, and Nenghai Yu. Recursive Histogram Modification: Establishing Equivalency Between Reversible Data Hiding and Lossless Data Compression. *IEEE Transactions on Image Processing*, 22(7):2775–2785, 2013.

ZHM07. Xunzhan Zhu, Anthony T.S. Ho, and Pina Marziliano. A new semi-fragile image watermarking with robust tampering restoration using irregular sampling. *Signal Processing: Image Communication*, 22(5):515–528, 2007.

ZHT$^+$07. X. Zhao, A.T.S. Ho, H. Treharne, V. Pankajakshan, C. Culnane, and W. Jiang. A Novel Semi-Fragile Image Watermarking, Authentication and Self-Restoration Technique Using the Slant Transform. In *Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2007. IIHMSP 2007.*, volume 1, pages 283–286, 2007.

ZPP10. Xian-Ting Zeng, Ling-Di Ping, and Xue-Zeng Pan. A lossless robust data hiding scheme. *Pattern Recognition*, 43(4):1656–1667, 2010.

ZQRF11. Xinpeng Zhang, Zhenxing Qian, Yanli Ren, and Guorui Feng. Watermarking With Flexible Self-Recovery Quality Based on Compressive Sensing and Compositive Reconstruction. *IEEE Transactions on Information Forensics and Security*, 6(4):1223–1232, 2011.

ZSN04. D. Zou, Y.Q. Shi, and Zhicheng Ni. A semi-fragile lossless digital watermarking scheme based on integer wavelet transform. In *IEEE 6th Workshop on Multimedia Signal Processing, 2004*, pages 195–198, 2004.

ZSNS06. D. Zou, Y.Q. Shi, Zhicheng Ni, and Wei Su. A Semi-Fragile Lossless Digital Watermarking Scheme Based on Integer Wavelet Transform. *IEEE Transactions on Circuits and Systems for Video Technology*, 16(10):1294–1300, 2006.

ZW08. Xinpeng Zhang and Shuozhong Wang. Fragile Watermarking With Error-Free Restoration Capability. *IEEE Transactions on Multimedia*, 10(8):1490–1499, 2008.

ZWQF11. Xinpeng Zhang, Shuozhong Wang, Zhenxing Qian, and Guorui Feng. Reference Sharing Mechanism for Watermark Self-Embedding. *IEEE Transactions on Image Processing*, 20(2):485–495, 2011.