We are IntechOpen, the world's leading publisher of Open Access books Built by scientists, for scientists

6,900
Open access books available

185,000
International authors and editors

200M
Downloads

Our authors are among the

154
Countries delivered to

TOP 1%
most cited scientists

12.2%
Contributors from top 500 universities



WEB OF SCIENCE™

Selection of our books indexed in the Book Citation Index in Web of Science™ Core Collection (BKCI)

Interested in publishing with us?
Contact book.department@intechopen.com

Numbers displayed above are based on latest data collected.
For more information visit www.intechopen.com



9

Audio Watermarking for Automatic Identification of Radiotelephone Transmissions in VHF Maritime Communication

Oleksandr V. Shishkin and Vitaliy M. Koshevyy
Odessa National Maritime Academy
Ukraine

1. Introduction

Audio watermarking (AW) corresponds to digital information imperceptibly embedded into the audio signal. AW for maritime VHF (Very High Frequency) communication is inspired first of all by the ability of implementation an automatic identification of radiotelephone transmissions in the channels of maritime (156…174) MHz mobile radio communication service. Applied to VHF radiotelephony, a watermarking system could overcome existing limitations, and ultimately increase safety and efficiency of maritime communication. The same application of AW may be implemented in the aeronautical (118…136) MHz mobile service. In the mentioned services analogue broadcasting channels with frequency/phase and amplitude modulation correspondingly are utilized.

For the meanwhile the identification of the sea vessels is realized by means of verbal calling of ship's call sign or numerical identification. However on account of different reasons such verbal identification may be absent, transmitted with delay, or understood with errors. This problem is illustrated in Fig. 1. Motor vessel "Arcona" transmits a certain message to all stations. But one of the receiving vessels missed the name and call sign of the transmitting ship, and another ship interpreted the name of transmitting ship as "Gargona" instead "Arcona".

It is obvious that false, incorrectly interpreted or delayed verbal identification negatively affects maritime navigation. Automatic identification could avoid misidentification and call sign confusion. Strictly speaking from the time the Global Maritime Distress and Safety System (GMDSS) (Brehaut, 2009) came in force in 1999, each radiotelephone exchange should be preceded by digital selective calling (DSC) on special calling channel 70 and appropriate acknowledge by means of DSC. After such calling procedures the radiotelephone transmission should be started on the assigned in DSC working channel. Meanwhile DSC and radiotelephone exchange are two independently executed by the navigational officer operations. Correct execution of these operations under Radio Regulation completely depends on human factor. In practice, however, DSC is often ignored, and navigators at once use radiotelephone channel 16. Especially this is typical for urgent communication. In such circumstances timely, clear and authentic identification is extremely necessary. Automatic identification would exclude the human factor and increase an efficiency of VHF radiocommunication and maritime safety in the whole.

Identification in DSC is produced by means of so called maritime mobile service identity (MMSI). MMSI is a unique combination of nine decimal digits. In binary representation MMSI occupies 36 bits sequence in DSC format. The same identification by means of MMSI may be applied to radiotelephone identification.

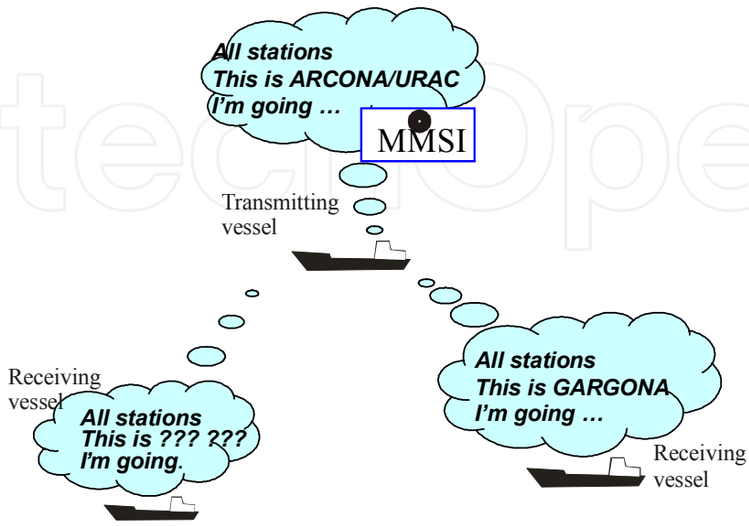


Fig. 1. Audio watermarking makes possible guaranteed identification of VHF maritime radiotelephony

Verbal identification doesn't protect against illegal radio transmission. Illegal transmissions are especially harmful on the VHF distress channel 16. Of course, violators are transmitting anonymously. Reliable identification of such transmissions could avoid the violation of radiotelephone regulation.

Another advantage of automatic identification becomes apparent in the ability of digital information inputting to another ships' navigational and information systems, for example ECDIS (Electronic Chart Display and Information System). ECDIS makes visualization of neighboring vessels in the range of VHF radio (i. e. approximately 30 nautical miles). However the transmitting vessel by no means is marked in an electronic map. Automatic identification would enable to mark on the electronic chart the transmitting vessel. Such an innovative function of ECDIS would be useful for clearing of current navigational environment. It is obvious that in such visual presentation navigator officer decision could be accepted more quickly and correctly. Such application of AW would again reduce risks of human factor demonstration.

One more application of AW is a covered information transmission in the special applications (for example, facing the threat of terrorist aggression).

It is essential that AW doesn't require altering an existing radio installation and operational procedures. AW identification keeps standard equipment and procedures. Only new telephone receiver (or headset) with embedded processor at the transmitter side and processor with mini-display switched to common audio output at the receiver side are to be mounted. Automatic identification starts right away press-to-talk switching and runs during all transmitting period independently from verbal signal occurrence. No additional time and frequency channel recourses are required.

2. Watermarking as communication problem

Watermarking may be examined in the frame of common communication problem (Cox et al., 2008), especially taking into account numerous algorithms of signal processing and technologies acquired in the field of conventional communication.

2.1 Watermarked communication over a channel with side information

Model of communication system with additive embedding of digital watermarks is presented in Fig. 2. Watermark signal w is formed on the base of embedded data m. Encoder may use information about carrier signal (or host signal) x, that is reflected with dotted line. Then carrier signal x is added by watermark w. Power σ_w^2 of w is limited by the acceptable level of introduced distortions of carrier signal because watermark w should be imperceptible on the background of carrier signal x.

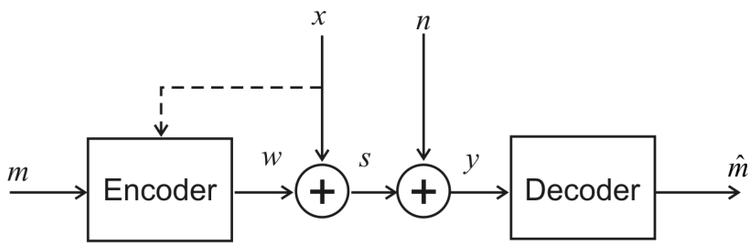


Fig. 2. Watermarked communication over a channel with side information

In the channel two interferences act against watermark w: the first interference is itself the carrier signal with the power σ_x^2, and the second one – a noise n with the power σ_n^2. Watermarking channel is characterised by its capacity - the maximum achievable code rate. Assuming the both interferences are white Gaussian noises the capacity C (bit/sample) of watermarked channel with noniformed encoder, when host signal is not available to encoder, is defined by formula:

$$C = \frac{1}{2}\log_2\left(1 + \frac{\sigma_w^2}{\sigma_x^2 + \sigma_n^2}\right). \quad (1)$$

Practically $\sigma_w^2 << \sigma_x^2$, and capacity is limited mainly by the host itself.

At the same time using information about the carrier signal x, it is possible to increase C (this is a case of informed encoder). An idea of informed encoder goes back to Kuznetsov & Tsybakov, 1974 and is known as writing in memory with defective cells. Gel'fand & Pinsker, 1980 and Costa, 1983 shown that assuming the host is known at the transmitter, the capacity is defined by the formula:

$$C = \frac{1}{2}\log_2\left(1 + \frac{\sigma_w^2}{\sigma_n^2}\right). \quad (2)$$

The Eq. (2) shows that carrier signal doesn't influence on watermark transmission and the capacity is determined only by the second noise, which is unknown at the encoder. Capacity

for such channel is increasing very much. The signal doesn't act as a noise source, that's why an informed encoding (i.e. "writing on dirty paper") is an attractive method for watermarking on account of potential capacity.

Noninformed encoder watermarking techniques exploit spread spectrum (SS) methods. In SS schemes the embedded bit flow is modulated by an SS sequence and added to the signal in the time or frequency domain. In schemes using SS the signal itself is seen as a source of interference and for reliable watermark restoration at the receiver the length of spreading sequence should be rather long to accumulate sufficient watermark energy. SS methods are traditionally considered as the most resistant against various attacks.

Capacity according Eq. (1) for SS watermarking is valid for assumption that the host signal is additive white Gaussian (AWGN) process. In practice, speech signal is highly correlated process and characteristics of SS watermarking may be remarkably improved. In paragraph 6 we consider adaptive whitening procedure for decreasing interfering influence of the host signal on watermark detection.

Informed encoding techniques are based on quantization the host signal directly or its certain transformation. The most popular method for this mode of embedding is quantization index modulation (QIM), proposed by Chen & Wornell, 2001. QIM-methods are free from the host signal interference, but commonly are more sensitive to attacks in watermarking channel.

Our investigations are based on classical communication approaches, applied to watermarking. It is known another view to the problem, for instance Hofbauer, et al., 2009 presented a blind speech watermarking algorithm that embeds the watermark data in the phase of non-voiced speech by replacing a certain voice segments on watermarked signal. However, the proposed method is based only on speech as a carrier signal and cannot involve any audio signals.

A comprehensive review of state-of-art methods for watermarking and data hiding is done by Moulin & Koetter, 2005. From the variety of watermarking method we focused on three candidates: SS, QIM and improved SS (ISS). The main goal of the paper consists in applying the modern communication technologies to audio watermarking.

2.2 Interferences in VHF radio channel

In this section we consider interferences which are important for watermarking in VHF analog radiochannel.

AW uses the common radiotelephone channel. The main interferences in through audio-radio-audio channel that affect AW are:

1. intersymbol interference (ISI) caused by low frequency circuits in the transceiver and multipass radio waves propagation;
2. flat amplitude fading;
3. external additive noise;
4. nonlinear distortions (clipping);
5. resampling and desinchronization.

Hofbauer & Kubin, 2006 proposed to take into account also Doppler effect that is actual for aeronautical applications.

Watermarking channel model is presented in Fig. 3.

Watermarking is concerned with the reliable transmission of information embedded into a host signal. The main difference from classical communication situation comes from the restriction of the host signal distortion. Digital watermarking can be viewed as a communication problem: information m to be sent from point A to point B is encoded into a signal w using information on host signal x. It is clear that making use of x calls for some time delay in x transmission. The time delay depends on complexity of processing at the encoder. But practically delay less then 100 – 200 msec in the master channel determines nothing but gives the ability to eliminate interfering influence of host on watermark signal w. Standard audio-radiotelephone channel in Fig. 3 is denoted C – D.

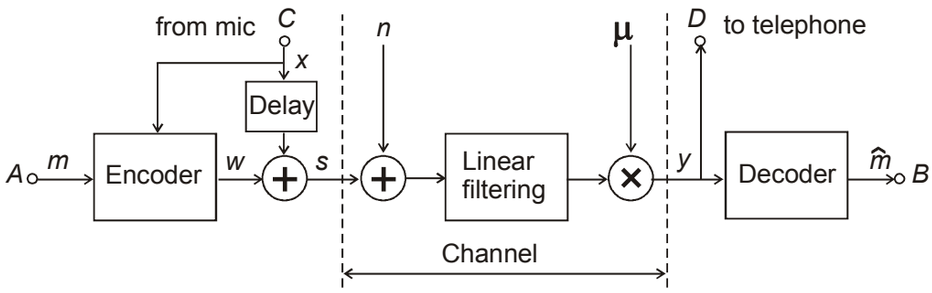


Fig. 3. Watermarking channel model

Watermarked signal $s = x + w$ is then passing through a common channel, which is unknown by nature. The embedded watermark should be reliably decodable even after further processing of the marked signal, which is also denoted as attack against the embedded watermark. Consider that malicious attacks are absent.

The attacks result unavoidable signal degradation. For robust watermarking we need restoration of embedded information m until speech communication in the master channel is possible. Another words watermarks robustness should monotonically fall with the quality of radio transmission in the master channel.

2.2.1 Intersymbol interference (ISI)

ISI forms distortions of a signal in which current symbol interferes with the previous one. Previous symbol has influence on the current symbol like noise, thus making communication less reliable. In the radio (or wireless) channels ISI is usually caused by multipath propagation. The transmitting medium in VHF radio communication is the atmosphere, in which radio signal is transferred by means of electromagnetic waves. The received electromagnetic signal is usually a superposition of a line-of-sight path signal and multiple waves coming from different directions. This phenomenon is known as multipath propagation. It is clear that reflected waves have to pass a longer distance and therefore arrive with a time-delay compared to the line-of-sight signal. The received signal is spread in time and the channel is said to be time dispersive. The time delays correspond to phase shifts in between superimposed waves. The phase shifts vary depending on frequency and signal frequency component may be cancelled or reinforced. This effect is known as

frequency selective fading and gives rise to notches in the frequency response of the channel.

Another physical cause of ISI is nonuniformity of frequency response of a channel. Analog low-frequency circuits of the transceiver are composed from reactive elements. These elements (including spurious effects) are bases for channel frequency band limitation. Frequency dependent elements cause nonuniformity of frequency response within audio signal spectrum. When frequency response is explicitly nonuniform within signal spectrum output signal highly differs from input one. Distortions caused by bandlimited low-frequency channel also represent ISI.

From the signal processing point of view the two physically different causes (presence of reactive elements in audio circuits and multipath radio wave propagation) lead to the same final result in the form of ISI.

For watermarking ISI may be simulated by linear filtering with appropriate frequency or impulse response. In Fig. 3 the two above mentioned sources of ISI are incorporated in one block denoted "Linear filtering".

2.2.2 Flat fading

Coming back to multipath propagation, one can analyze a variant when the different path lengths are very similar compared to the wavelengths of the signal components. Then the phase variations between components will be small and they will all undergo very similar amounts of cancellation or reinforcement. This case is usually termed flat fading.

In watermarking flat fading is simulated by amplitude scaling attacks. In Fig. 3 flat fading is shown as multiplicative interference μ.

2.2.3 Additive noise

Additive noise is imposed onto the signal during transmission. The noise results from thermal noise in electronic circuits, from atmospheric noise or from other radio stations. Quantization noise from analog-to-digit converter may be attributed to additive noise. Commonly recognized model of an additive noise is additive white Gaussian noise, denoted in Fig. 3 by n.

2.2.4 Nonlinear distortions

Nonlinear distortions appear in amplitude limitations caused, for example, by the overload in audio circuits. Overload arises from redundant power of transmitting station. The simplest model of nonlinear distortions is clipping. AW in any case should be resistant against such distortions. Source of nonlinear distortion is not shown in Fig. 3.

2.2.5 Desynchronization and resampling

At the transmitter and receiver sampling processes are not synchronized. It means that sampling instants are mutually shifted. Consider sampling frequencies are equal at the transmitter and receiver. At the receiver beginning of watermark is unknown. For

watermark restoration beginning of watermark should be first detected and then all decision points are counted from the starting point. Analog radiotelephone channel by all means leads to resampling and loss of the watermark beginning. Desynchronization and resampling attacks are not reflected in Fig. 3.

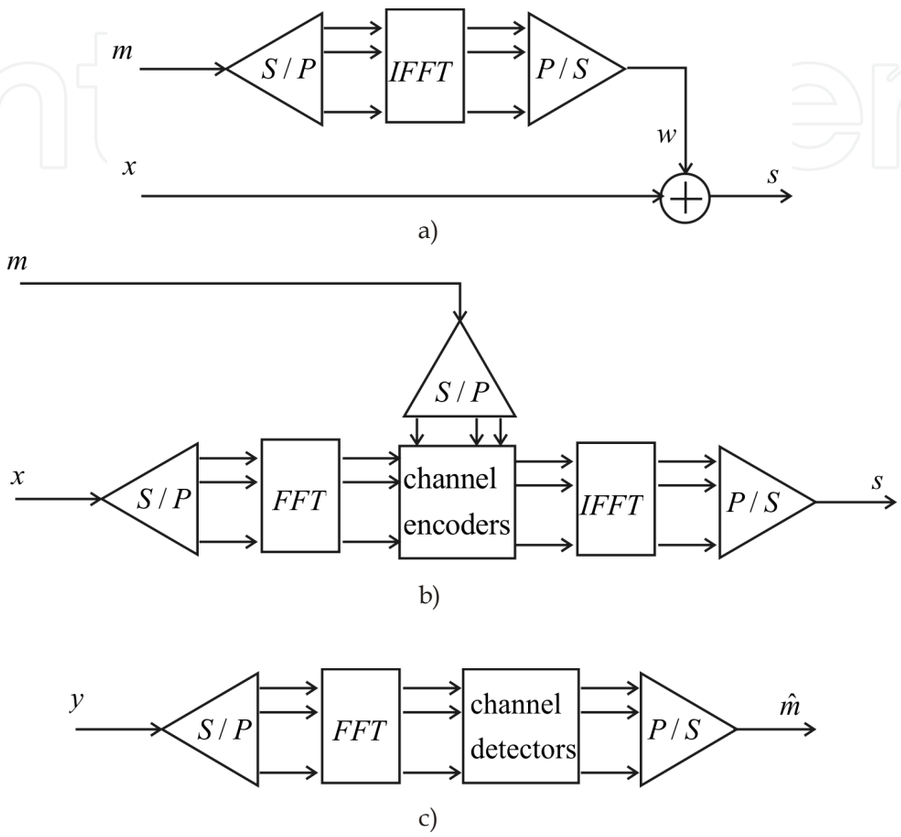


Fig. 4. OFDM application for watermarking: a) noninformed encoding;
b) informed encoding; c) decoding

3. OFDM for watermarking

Orthogonal frequency division multiplexing (OFDM) is well known multi-carrier modulation method and is used in various wireless communication systems (Ipatov, 2005). It has been shown to be an effective technique to combat multipath fading in wireless channels.

3.1 OFDM based watermarking schemes

In basic OFDM scheme data symbols modulate a parallel collection of regularly spaced sub-carriers. OFDM is simple to use on channels with time delay spread or, equivalently, frequency selectivity. OFDM converts one frequency selective channel into a parallel collection of frequency flat sub-channels. Techniques that are appropriate for flat fading channels can then be applied in a straight forward fashion to every sub-channel.

A general system for SS watermarking based on OFDM principle is shown in Fig. 4 a). Sequence of message bits m first is split in serial-to-parallel (S/P) block into some "slow" flows. Relation between a dimension of inverse fast Fourier transform (IFFT) and a number of slow flows depends on what Fourier coefficients are subjected for watermarking. So that some of inputs of IFFT block may be set to zeros. Then parallel-to-serial (P/S) block combines slow flows into one sequence which represents watermark it the time domain. Commonly SS methods use a certain type of transform (discrete cosine transform (DCT), discrete Fourier transform (DFT), Wavelet, etc.) for subsequent watermarking of transformation coefficients.

Application of any transform demands storing of carrier signal and strictly speaking leads to some delay in signal transmission. OFDM scheme produces inherently the same watermarking of fast Fourier transform (FFT) coefficients without any delay. Encoder turns out really noninformed.

General system for informed OFDM encoding is presented in Fig. 4 b). Signal x is splited into slow flows which are subjected to FFT. Message flow m is splited into some, suppose B, $(B < N/2)$ slow flows. Channel encoders use B Fourier coefficients for watermarking independently in each channel. In the simple case one bit may watermark one coefficient. For more complex variants one embedded bit may be distributed among $L > 1$ coefficients. In general NL samples of x are needed for embedding B message bits. Algorithms for each channel encoders are identical. Watermarked coefficients and all the rest undisturbed coefficients are then used for IFFT. Again P/S block combines slow flows into one sequence s in the time domain.

Watermarked signal s to resist against intersymbol interference may be added with prefix s_p (see below) so the watermarked signal becomes $[s_p, s]$. Prefixed signal presents so called OFDM symbol and is then transmitted through the channel.

At the receiver (Fig. 4 c) OFDM symbol is primarily cleared from the prefix, which is mostly corrupted by ISI. This operation is not shown in the figure. Then signal y is splited into N flows which are transformed in Fourier coefficients. These coefficients are processed according to demodulation algorithm for extracting a watermark message bits $\hat{m}$. Receiving scheme is general for informed and noninformed encoding.

Attractive features of OFDM-like watermarking are good vectorisation for encoding and decoding algorithms and application of standard FFT and IFFT procedures.

3.2 Resistance to ISI

Let us show how to apply the main principles of OFDM for resistant to ISI watermarking.

According to inverse DFT signal block x_n, $n = 0,1,\ldots,N-1$ may be composed from N harmonics with complex amplitudes $\dot{X}_k$, $k = 0,1,\ldots,N-1$.

$$x_n = \frac{1}{N}\sum_{k=0}^{N-1} \dot{X}_k \exp\left(j\frac{2\pi nk}{N}\right), \quad n = 0,1,\ldots,N-1. \tag{3}$$

At the decoder on account of ISI we have harmonics on the same frequency grid, but with another complex amplitudes $\dot{Y}_k \neq \dot{X}_k$, where $\dot{Y}_k$ are obtained from DFT:

$$\dot{Y}_k = \sum_{n=0}^{N-1} y_n \exp\left(-j\frac{2\pi nk}{N}\right), \quad k = 0,1,\ldots,N-1. \tag{4}$$

According to OFDM principle each harmonic should be cyclically extended with P samples. Then we obtain so called OFDM symbol:

$$x'_n = \frac{1}{N}\sum_{k=0}^{N-1} \dot{X}'_k \exp\left(j\frac{2\pi nk}{N}\right), \quad n = 0,1,\ldots,N+P-1, \tag{5}$$

where $\dot{X}'_k$ - complex amplitudes undetermined for the present.

It obvious that $x'_{N+i} = x'_i, \quad i = 0,1,\ldots,P-1.$

However we couldn't insert $N+P$ samples instead of N samples without sampling frequency alteration. We are forced to utilize $N+P$ samples x'_n from Eq. (5) instead of N samples x_n from Eq. (3) plus subsequent P samples from the future block. Prefix results in the host signal distortions and serves as a penalty for ISI decreasing. The length of prefix comes from the channel impulse response. Reasonable P may be accepted to suppress ISI while keeping introduced distortions.

Mathematically equations (5) presents an overdetermined system with $N+P$ equations and N unknowns $\dot{X}'_k$.

For the least squares criteria $\min\|x_n - x'_n\|$ mathematic methods are well designed and implemented in MatLab.

Solution of system (5) is inaccurate in general and consists from complex numbers $\dot{X}'_k$, $k = 0,1,\ldots,N-1$. Therefore samples x'_n may come up to complex values also. Only if $\dot{X}'_k = \dot{X}'^{*}_{N-k}$, $k = 1,\ldots,N/2-1$ and $\dot{X}'_0, \dot{X}'_{N/2}$ are both real, the sequence x'_n is guarantied to be real.

To obtain real values x'_n let us represent system (5) in trigonometric form. Denote $\dot{X}'_k = a_k + jb_k$ in Eq. (5). After evident transformation one may get the system in required form:

$$x'_n = \frac{2}{N}\left(\frac{a_0}{2} + \sum_{k=1}^{N/2} a_k \cos\frac{2\pi}{N}kn - b_k \sin\frac{2\pi}{N}kn\right), \quad n = 0,1,\ldots,N+P-1 \tag{6}$$

As before we have $N+P$ equations and N unknowns: a_0, $(a_k, b_k), k = 1,2,...,N/2-1$, $a_{N/2}$. Least squared solution will be in real field numbers and sequence the x'_n is assured to be real also.

Coefficients $\dot{X}'_k$, or part of them, are subjected for watermarking. In general we get the watermarked coefficients:

$$\dot{S}_k = \dot{X}'_k + \dot{W}_k, \quad k = 1,2,...,B. \tag{7}$$

In Eq. (7) it is supposed that watermarked coefficients are from 1 to B.

First N samples of watermarked sequence are calculated by means IDFT: $s_n = \mathrm{IDFT}\{\dot{S}\}$, $n = 0,1,\ldots,N-1$ and supplemented with repeated prefix.

Because of ISI received block $y = [y_0, y_1, ..., y_{P+N-1}]$ even providing zero additive noise differs from transmitted block. Initial samples are especially corrupted by ISI. For processing decoder removes the first P samples and computes coefficients $\dot{Y}_k = \mathrm{DFT}\{y\}$, utilising the last samples $y = [y_P, y_{P+1}, ..., y_{P+N-1}]$, which are free from ISI.

Prefix appending results in matching linear $y = s * h$ and cyclic $\tilde{y} = \tilde{s} * \tilde{h}$ convolutions at interval $[P+1, N+P]$. Here $\tilde{s}, \tilde{h}$ - are periodic sequences which are formed from the sequences $[s_0, s_1, ..., s_{N-1}]$, $[h_0, h_1, ..., h_{P-1}, 0, 0, ..., 0]$ correspondingly and the second sequence is added by zeros up to N samples.

If $\dot{Y}, \dot{S}, \dot{H}$ - are DFTs of $\tilde{y}, \tilde{s}, \tilde{h}$, then

$$\dot{Y} = \dot{S}\,\dot{H}. \tag{8}$$

In the last Eq. (8) $\dot{H}$ - is the frequency response of general channel.

According to basic idea of OFDM an audio signal can be split into the some of sub carriers on frequencies $f_0, f_1, ..., f_{N-1}$. Every sub carrier has its own complex amplitude, say $\dot{X}_i$. The amplitudes vary from slot to slot and are constant within every time slot.

From point of view of watermarking every sub carrier forms separate sub channel, and every channel operates independently from each other. Amplitudes $\dot{X}_i$ are subjected to watermarking. Assume they are altered to $\dot{S}_i$ according certain algorithm. Since sub carriers are orthogonal the amplitudes $\dot{S}_i$ will not have influence on each other. Composed watermarked audio may by presented in the form:

$$\dot{S}(t) = \sum_{i=1}^{M} \dot{S}_i \exp(j2\pi f_i t). \tag{9}$$

Every sub channel occupies a narrow frequency band. It is reasonable to assume that within one sub channel frequency response of the general channel is constant.

Thanks to prefix ISI is eliminated and received complex amplitude in sub channel will be defined by Eq. (8).

For slow fading it is considered $\dot{H}(j2\pi f_i) = const$ within one time slot.

4. Quantization Index Modulation (QIM)

Chen & Wornell, 2001 introduced a class of data-hiding codes known as dither modulation codes, or quantization index modulation (QIM) codes. These methods are based on quantization techniques.

4.1 Scalar and complex QIM

The simplest implementation of quantization-based watermarking employs scalar quantizer for embedding one bit into one host sample. The watermarking rule for this case is

expressed through the quantization function $s = Q(x)$, where scalar quantization function may be presented in the form:

$$Q(x,m) = \Delta \text{round}\left(\frac{x}{\Delta} + \frac{m}{2}\right) - \Delta\frac{m}{2}. \quad (10)$$

In Eq. (10) denoted: Δ - quantization step, $m = \{0, 1\}$ - embedded bit, $\text{round}(\cdot)$ - rounding operation.

Quantization step is chosen depends on distortions-robustness trade-off.

Scalar QIM translates real numbers x into lattices $\Lambda_m = \Delta Z - m\Delta/2$, Z - is set of integer numbers.

The QIM decoder operates as a minimum-distance decoder. It finds the quantizer node closest to y and forms the estimation of extracted bit

$$\hat{m} = \arg\min_{m\in\{0,1\}} \left\| y - Q(y,m) \right\|. \quad (11)$$

Let us introduce quantization on the complex plain and denote it QIM2. Complex quantization function for QIM2 is written in the form:

$$\dot{s} = \tilde{\Delta}\text{round}\left(\frac{\dot{x}}{\tilde{\Delta}} + \frac{m}{2}(1+j)\right) - \tilde{\Delta}\frac{m}{2}(1+j), \quad (12)$$

where $j = \sqrt{-1}$.

Step of quantization $\tilde{\Delta}$ represents in general a complex number. Rounding of complex magnitude is done independently according to real and imagynary axes.

Complex quantization QIM2 is illustrated in Fig. 5. QIM2 uses two-dimensional lattices

$$\Lambda_0 = \tilde{\Delta} Z, \ \Lambda_1 = \tilde{\Delta}(Z + 1/2), \quad (13)$$

where $Z = ...,-2,-1,0,+1,+2,...$ - set of integer numbers.

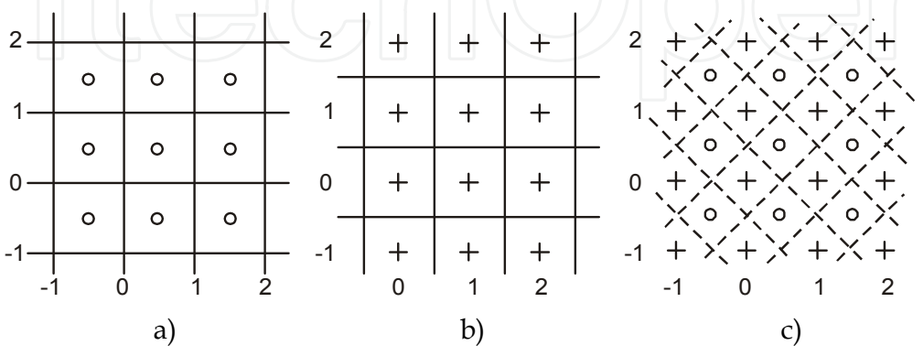


Fig. 5. Lattices on the complex plain: a) lattice for $m = 1$, b) lattice for $m = 0$, c) partition to decision areas

Advantage of QIM2 over scalar QIM consist in increasing the of distance between the nearest concurring decision points. It is possible to show that, assuming equal distortions the minimal distance is $\sqrt{2}/2$ times greater for QIM2 procedure comparatively to scalar QIM (see Fig. 5).

4.2 Invariance to amplitude scaling and phase shift

The main drawback of QIM is sensitivity to amplitude scaling and filtering.

Perez-Gonzalez et al., 2005 proposed techique for images processing against value-metric scaling attack, named as rational dither modulation (RDM). The main idea of RDM is snaping of quantization steps to watermarked and received signals at the transmitter and receiver correspondingly. For the first order for RDM scheme steps quantization for the current samples X_k and Y_k are produced on the base of previous samples S_{k-1} and Y_{k-1}. Assuming noise absence, the influence of constant multiplier μ in the channel is fully eliminated on decoding process.

This scheme works until $|S_{k-1}| \neq 0$. Performance of the first order RDM scheme may by improved by high order schemes. Stepsize estimation at the transmitter is produced on the base of l previous watermarked samples and is given by the p norm of vector S:

$$g = \left(\frac{1}{l} \sum_{i=1}^{l} |S_{k-i}|^p \right)^{\frac{1}{p}}. \tag{14}$$

Analogous procedure is produced at the receiver with vector Y.

Let us extend idea of double stepsize calibration on complex quantization that will be useful for enhancing watermark resistance to filtering. For this purpose apply RDM approach on the case of complex multiplicative interference $\dot{\mu} = \mu \exp(-j\varphi_0)$. This interference adds constant unknown phase shift φ_0. We want to quantize complex amplitudes on a plain lattice invariantly to this shift. For that it is necessary to make QIM process transparent not only to amplitude scaling but to phase alterations also.

Suppose vector $\dot{S}$ presents complex amplitudes of narrowband signal. Passing the channel all amplitudes $\dot{S}$ changes their amplitudes by μ : $|\dot{Y}_i| = \mu |\dot{S}_i|$ and corresponding phases by φ_0 : $\arg(\dot{Y}_i) = \arg(\dot{S}_i) + \phi_0$. Phase of the resulting vector at the transmitter is given by

$$\phi_S = \arg\left(\sum_{i=1}^{l} \dot{S}_i \right). \tag{15}$$

Thanks to narrowband nature phase of resulting vector $\dot{Y}$ at the receiver will be turned on phase ϕ_0 compared to transmitter: $\phi_Y = \phi_S + \phi_0$. Adding phase multiplier $\exp(-j\phi_S)$ in Eq. (14) we get complex estimation for quantization step.

Appropriate equations in vector form are presented below:

$$\mathbf{G}_{k-1} = \mathbf{g}_{k-1} \exp(j\mathbf{\Phi}_{k-1}), \tag{16}$$

$$\mathbf{g}_{k-1} = \left(\frac{1}{l} \sum_{i=1}^{l} |\mathbf{S}_{k-i}|^{p} \right)^{\frac{1}{p}} \tag{17}$$

$$\mathbf{\Phi}_{k-1} = \arg\left(\sum_{i=1}^{l} \mathbf{S}_{k-i} \right) \tag{18}$$

Vector for step quantization in Eq. (12) is then given by the relation

$$\tilde{\Delta}_{k-1} = \Delta \, \mathbf{G}_{k-1} . \tag{19}$$

where Δ is certaine stepsize chosen apriory.

The same ralations shold be used at the receiver with the substitution vector $\mathbf{Y}_{k-i}$ instead of $\mathbf{S}_{k-i}$. Note that all bold-marked vectors have length B. At the receiver detection of embedded bits is performed by using a minimum Euclidian distance rule, i.e.

$$\hat{\mathbf{m}} = \arg\min_{\mathbf{m} \in 0,1} \left\| Q\left(\mathbf{Y}_k, \mathbf{G}_{k-1}, \mathbf{m} \right) - \mathbf{Y}_k \right\| . \tag{20}$$

Relations (16) - (20) make possible to eliminate flat fading and realize QIM process fully imperceptible to slowly amplitude scaling and phase shift.

From Eq. (8) it is clear that invariant amplitude scaling and phase shift procedure, abbriviate it as IAP, can be applied to each narrowband channel. Multi channel encoder implementation is presented in Fig. 6.

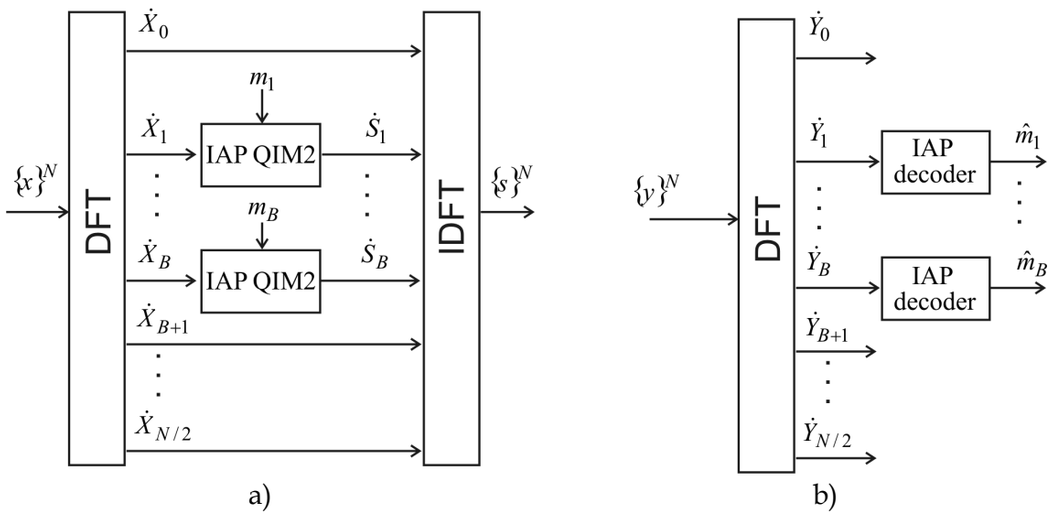


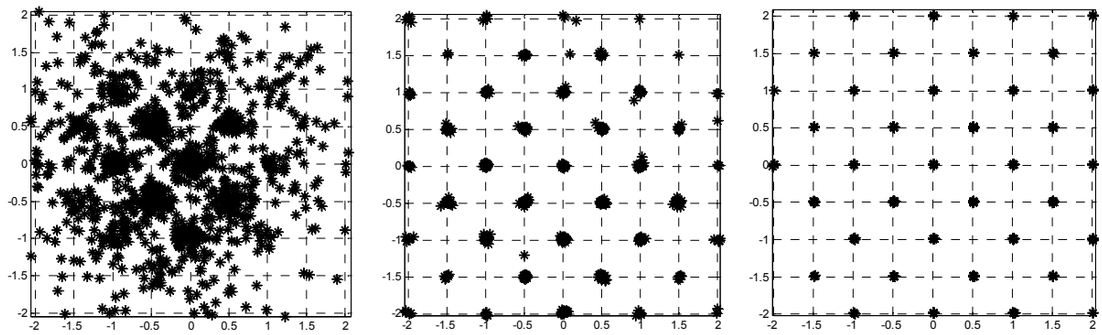
Fig. 6. OFDM invariant to amplitude scaling and phase shift QIM2 system:
a) transmitter; b) receiver

Coming through the channel signal is subjected to linear filtering. Thanks to prefix the received signal after linear filtering may be considered in the frequency domain according to

Eq. (8). At the receiver prefix $[y_1, y_2, ..., y_P]$ is removed and the remaining samples $[y_1, y_2, ..., y_N]$ are used for performing DFT. Then decoding IAP procedures are performed under coefficients $\dot{Y}_1, \dot{Y}_2, ..., \dot{Y}_B$ for detecting embedded bits $\hat{m}_i$, $i = 1, ..., B$ in each channel

In Fig. 7 simulation results are presented for filtering attack. For channel simulation Butterworth low pass filter of order 2 an cut off frequency 0.3 was chosen. Function representing that filter in MatLab is: [b,a]=butter(2,.3). Length of impulse response for that filter is 8. Additive noise is absent. Number of watermarked channel is $B = 8$.

It is seen that even for zero prefix received complex amplitudes $\dot{Y}$ are scattered because of ISI influence (Fig. 7 a). Increasing P leads to concentration of $\dot{Y}$ around centroids $\dot{S}$, and for $P = 8$ dispersion is nearly zero: $\dot{Y} = \dot{S}$.



a) b) c)

Fig. 7. Influence of prefix on scattering for OFDM IAP QIM2 algorithm:
a) no prefix $P = 0$; b) moderate prefix $P = 4$; c) full prefix $P = 8$

5. Improved Spread Spectrum (ISS)

Malvar & Florencio, 2003 introduced ISS method for robust watermarking. In spite of the title ISS radically distinguishes from common SS due to utilization of information about carrier signal. When compared with traditional SS, the signal doesn't act as noise source. Thanks to that ISS encoding algorithm refers to informed encoding and may be treated as binary QIM. The main idea of ISS is to look ahead across the carrier signal and relying on it generate the appropriate watermark signal. Just as for standard SS chip sequence $\mathbf{u}$ is used but with the coefficient $\mu(\tilde{x}, b)$:

$$\mathbf{s} = \mathbf{x} + \mu(\tilde{x}, m)\mathbf{u}, \tag{21}$$

where $\tilde{x} = (\mathbf{x}, \mathbf{u})$, $m = \{-1, 1\}$ - embedded bit.

Here inner product is defined as:

$$(\mathbf{x}, \mathbf{u}) = \sum_{i=1}^{L} x_i u_i . \tag{22}$$

The main idea of ISS is to generate watermark vector $\mathbf{w} = \mu(\tilde{x}, m)\mathbf{u}$ in such mode that inner product $(\mathbf{s}, \mathbf{u})$ would give the value not less than certain threshold ρ if $m = 1$ and not

more than $-\rho$ if $m = -1$. It is obvious that there are situations when inserting of watermark signal is not needed at all. In this case distortions due to watermarking are absent. When do the modification of carrier signal is necessary, total correction expressed by the relation $\tilde{w} = \rho m - \tilde{x}$ is distributed along the carrier signal.

Taking into account that after embedding process according to Eq. (21) the watermarked amplitude may take negative value, the following algorithm for calculating $\mathbf{w}$ was applied:

$$\mathbf{w} = \begin{cases} \tilde{w}\mathbf{u}^- / \left\|\mathbf{u}^-\right\|, & \text{if} \quad \tilde{w} \geq 0, \\ \tilde{w}\mathbf{u}^+ / \left\|\mathbf{u}^+\right\|, & \text{otherwise} \end{cases}. \tag{23}$$

where symbol $\|\cdot\|$ denotes unit vector norm.

Sequences $\mathbf{u}^+ = \{0,1\}$ and $\mathbf{u}^- = \{0,-1\}$ are composed from sequence $\mathbf{u}$ according the following rules:

$$u_i^+ = \begin{cases} 1, & \text{if} \quad u_i = 1, \\ 0, & \text{otherwise} \end{cases} \quad u_i^- = \begin{cases} -1, & \text{if} \quad u_i = -1, \\ 0, & \text{otherwise} \end{cases} \tag{24}$$

Eq. (23), (24) eliminate in any case a negative amplitude values for watermarked signal according Eq. (21).

Detected bit is restored by means of sign function

$$\hat{m} = \text{sign}\left(\tilde{y}\right) \tag{25}$$

where, $\tilde{y} = \left(\mathbf{y}, \mathbf{u}\right)$.

Comparative detection characteristics for ISS and SS according Shishkin, June 2008 are presented in Fig. 8. Characteristics are plotted as error probability function versus watermark-to-signal ratio (WSR) and watermark-to-noise ratio (WNR) both expressed in dB. Graphics are plotted for identical parameters signal-to-noise ratio (SNR) and WSR accordingly. Teoretical bounds, when host signal is completely availablee at the receiver, i.e. nonblind watermarking are shown with dashed lines.

Almost vertical slope of $p_{er}(\text{WSR}, \text{SNR} = \text{const})$ is explained by the independency of watermarking channel capacity from the carrier signal (see Eq. (2)). Gain for ISS method is within (15 … 20) dB in comparison to SS Fig. 8 a)).

It is worth to notice that OFDM-like processing is completely applicable to ISS. Characteristics in Fig. 8 are given for zero prefix.

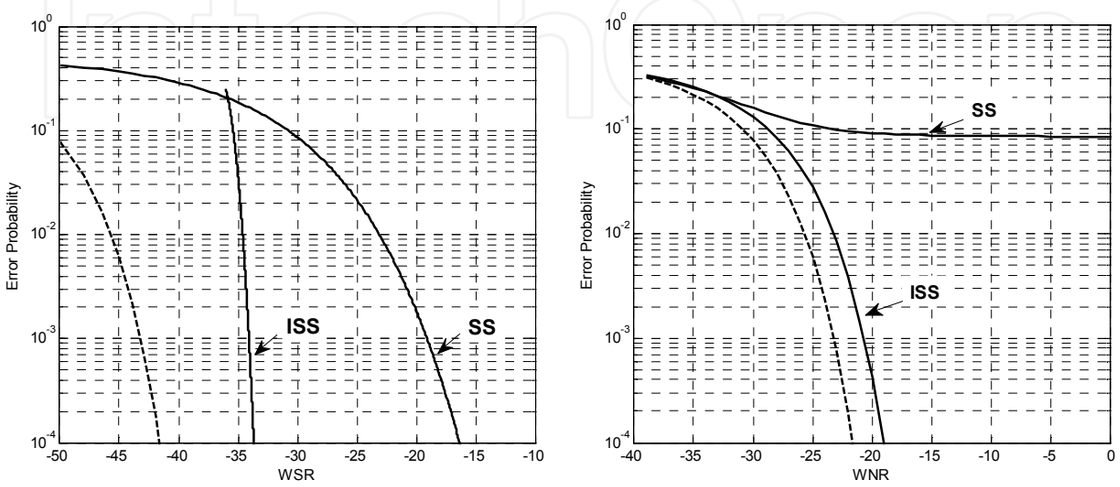
6. Adaptive cancelling of carrier signal at the receiver

SS-based watermarking algorithm embeds one bit of information in a vector $\mathbf{s}$ of L samples:

$$\mathbf{s} = \mathbf{x} + \sigma_w \, m \, \mathbf{u} \, , \tag{26}$$

where σ_w is wanted root mean square deviation of watermark, $m = \{-1, 1\}$ - information bit to be embedded, $\mathbf{u} = [u_1, u_2, ..., u_L]$ - binary pseudo random sequence, $u_i = \{-1, 1\}$.

If the channel modeled as additive noise, the received signal is: $\mathbf{y} = \mathbf{s} + \mathbf{n}$.



a) b)

Fig. 8. Comparative error probability functions for ISS and SS methods: a) p_{er} versus WSR, $SNR = 20$ dB, b) p_{er} versus WNR, $WSR = -30$ dB

Detection at the receiver is performed by the correlator that computes inner product

$$\tilde{y} = (\mathbf{y}, \mathbf{u}) = (\mathbf{x}, \mathbf{u}) + \sigma_w mL + (\mathbf{n}, \mathbf{u}). \quad (27)$$

Detected bit is estimated according to Eq. (25). One can see that interferences for watermark are terms $\tilde{x} = (\mathbf{x}, \mathbf{u})$ and $\tilde{n} = (\mathbf{n}, \mathbf{u})$ in Eq. (27). Suppose vectors $\mathbf{x}$ and $\mathbf{n}$ are uncorrelated random processes. Therefore terms in Eq. (27) $\tilde{x}$, $\tilde{n}$ grows proportionally $\sqrt{L}$, meanwhile useful term $\sigma_w mL$ is proportional to L. Processing gain is $\sqrt{L}$. It is possible to yield desired probability of detection through the appropriate chip length L.

Another possibility for achieving the goal appears when $\mathbf{x}$ represents a correlated process. Practically x is a really highly correlated process. And just this process has a maximal influence on watermark.

In communication optimal receiving algorithms in the presence of correlated noise are well developed (Van Trees, 1968). Scheme for optimal receiver on the background correlated noise is based on whitening filter (WF) and presented in Fig. 9. WF is based on predictor and forms at the output an error signal $e(i)$ between an actual sample and predicted one. For good predictor $e(i)$ looks like white noise with less power compared to power of input signal $y(i)$.

Verbal signal is a nonstationary random process and it requires adaptation of transfer function. For WF implementation let us apply linear prediction method. Basic principle of linear prediction consists in presentation of predicting sample through the linear combination of previous samples. Weighting coefficients in the linear combination are calculated on the basis of mean squared error minimization for prediction, i.e. differences between signal samples and theirs predicted values.

Linear prediction method in the view of so called linear predictive coding (LPC) is widely used in the audio compressing algorithms. LPC algorithm assumes partition of audio signal on frames of duration approximately 20 msec. For every segment weighting coefficients of WF, which would minimize mean squared error of prediction are calculated. Prediction at step i is expressed through the preceding samples:

$$y_{pr}(i) = h_1 y(i-1) + h_2 y(i-2) + ... + h_p y(i-p). \quad (28)$$

Prediction error comes to

$$e(i) = y(i) - y_{pr}(i) = \sum_{k=0}^{p} h_k y(i-k). \quad (29)$$

Coefficients h_k, $k = 1,2,...,p$ in Eq. (29) are subject of adaptation, $h_0 = 1$.

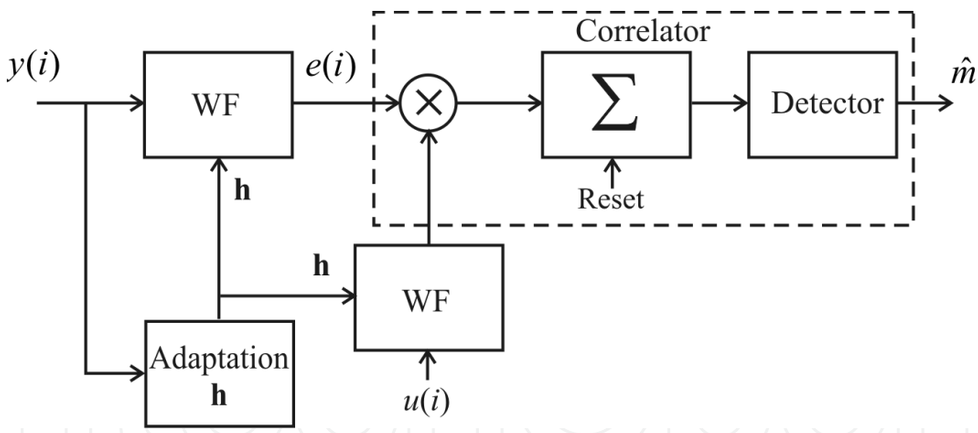


Fig. 9. Optimal receiver for watermark on the background of correlated noise

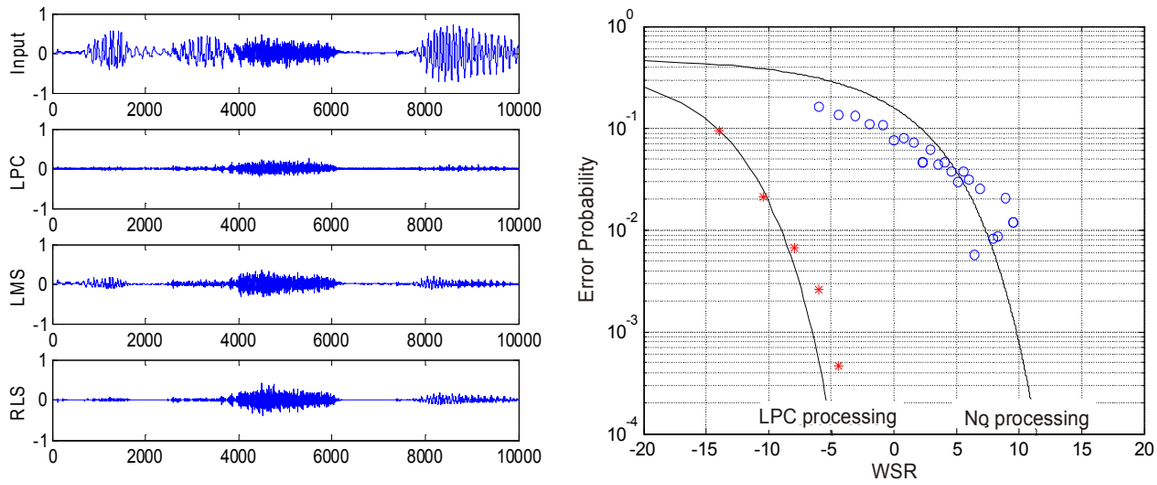
Algorithm for finding coefficients h_i is well elaborated mathematically. It is based on Yule-Walker equation and computing procedure by the Levinson-Durbin algorithm (O'Shaughnessy, 2000). In MatLab function lpc(y,p) finds the coefficients of a p -order linear predictor (finite impulse response filter) that predicts the current value of the real-valued time series y based on past samples.

LPC algorithm is block and applies the samples from fixed time interval. During filtration coefficients of WF doesn't vary within the frame. Coming to next frame the coefficients

should be recalculated. Other prediction procedures may use continuous adaptation algorithms, for example, Least Mean Square (LMS) or Recursive Least Square (RLS) algorithm. Shishkin, October 2008 simulated above mentioned algorithms for SS-watermarked speech signals (Fig. 10 a)). In Fig. 10 a) time axes are marked in sample numbers, assuming sampling frequency $F_s = 22050$ Hz , WF order $p = 7$.

Waveforms shows that prediction error is less for LPC algorithm compared to LMS and RLS. Time segments for samples 1 – 2000, 2000 – 4000 and 8000 – 10000 correspond to vowel sounds and have quite negligible prediction error because appropriate signal is highly correlated. On the other hand consonant speech sound (samples 4000 – 6000) is closer to white noise and that's why it is predicted worse.

Comparative detection characteristic for SS watermarking in AWGN channel are presented in Fig. 10 b). Watermarking was executed in the time domain. It is seen that additional processing at the receiver effectively suppress correlated speech signal. Processing gain makes approximately 15 dB.



a) b)

Fig. 10. Simulation results for adaptive carrier signal cancellation: a) signal waveforms after whitening according LPC, LMS, RLS algorithms; b) error probability as a function of WSR (Shishkin, October 2008)

7. Conclusion

Proposed OFDM technology application to QIM watermarking makes possible to resist against intersymbol interference, that is induced by multipath propagation and bandlimited nature of VHF radiotelephone channel. OFDM-QIM integration makes QIM watermarked signal to be invariant against amplitude scaling and phase shift. Reasonable prefix length about $P = 2...4$ to cancel ISI is acceptable for the total OFDM symbol size about 500 samples. The main restricted factor is reliable estimation for step quantization on the background of additive noise. One of the possible ways to resist against noise is one bit distribution on numerous samples, i.e. application of the principle

one bit – many samples (or coefficients) instead of principle one bit – one sample (coefficient).

Improved SS watermarking inherently resist to amplitude scaling. Noise immunity may be achieved by means of exchange embedding rate and noise robustness. For existing radiotelephone channel of frequency band (300 … 3000) Hz and signal-to-noise ratio about 15 dB realistic embedding rate forms about 60 bit/sec. This rate is quite sufficient for reliable identification. Presently ISS watermarking appears to be the most acceptable method.

Traditional SS method with additional processing at the receiver gives about 40 bit/sec rate. Absolute advantage of this method is absence of delay and simple encoding at the transmitter. OFDM-like pre-processing procedure makes possible to watermark in the frequency domain without any delay for transmitting signal.

8. References

Brehaut, D. (2009). *GMDSS: A User's Handbook* (Forth edition), Adlard Coles Nautical, ISBN 978-1408114933, London

Chen, B. & Wornell, G. (2001). Quantization index modulation: a class of provably good methods for digital watermarking and information embedding. *IEEE Transactions on Information Theory*, Vol. 47, No. 4, pp. 1423-1443

Costa, M. (1983). Writing on dirty paper. *IEEE Transactions on Information Theory*, Vol. IT-29, pp. 439 – 441

Cox, I.; Miller, M.; Bloom, J.; Fridrich, J. & Kalker, T. (2008). *Digital Watermarking and Steganography*, (Second edition), Morgan Kaufmann Publishers, ISBN 978-0-12-372585-1, Burlington, MA, USA

Gel'fand, S. & Pinsker, M. (1980). Coding for channel with random parameters. *Problems of Control and Information Theory*, Vol. 9, No.1, pp. 19 – 31

Hofbauer, K. & Kubin, G. (2006). Aeronautical voice radio channel modelling and simulation—a tutorial review, In: *Proceedings of the International Conference on Research in Air Transportation (ICRAT)*, Belgrade, Serbia, Available from http://www3.spsc.tugraz.at/people/hofbauer/papers/ Hofbauer_ICRAT_2006.pdf

Hofbauer, K. et al. (2009). Speech watermarking for analog flat-fading bandpass channels, *IEEE Transactions on Audio, Speech, and Language Processing*, 2009, Vol.17, No.8, pp. 1624 - 1637, ISSN 1558-7916

Ipatov, V. (2005). *Spread Spectrum and CDMA: Principles and Applications,* John Wiley & Sons, Ltd, ISBN 0-470-09178-9, Chichester, England

Kuznetsov, A. & Tsybakov, B. (1974). Coding in a Memory with Random Parameters. *Probl. Peredachi Inf,* Vol. 10, No.2, pp. 52-60, UDC 621.391.15

Malvar, H. & Florencio, D. (2003). Improved Spread Spectrum: A New Modulation Technique for Robast Watermarking, *IEEE Transactions on Signal Processing*, Vol.51, No.4, pp.898 – 905

Moulin, P. & Koetter, R. (2005). Data-Hiding Codes. *Proceedings of the IEEE*, Vol.93, No.12, pp. 2083 – 2126

O'Shaughnessy, D. (2000). *Speech communication: human and machine,* (Second edition), IEEE, Inc. New York, ISBN 0-7803-3449-3

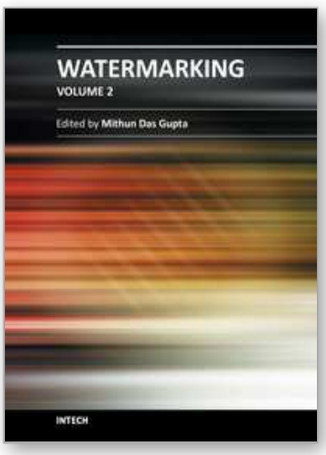
Perez-Gonzalez, F. et al. (2005). Rational Dither Modulation: A High Rate Data-Hiding Method Invariant to Gain Attacks. *IEEE Transactions on Signal Processing*, Vol.53, No.10, pp.3960–3975

Shishkin, A. (June 2008). Digital Watermarks with Spectrum Spreading for Audio Signals Using the Signal Carrier Information. *Radioelectronics and Communication Systems,* Vol. 51, No.6, pp.308-315, ISSN 0735-2727

Shishkin, A. (October 2008). Adaptive Algorithms Application in Sound Steganographic Systems with Signal Spectrum Broadening. *Radioelectronics and Communication Systems,* Vol.51, No.10, pp.524-530, ISSN 0735-2727

Van Trees, H. (1968). *Detection, Estimation, and Modulation Theory*, (First edition), John Wiley & Sons Inc, ISBN 978-0471899556

IntechOpen



Watermarking - Volume 2

Edited by Dr. Mithun Das Gupta

ISBN 978-953-51-0619-7
Hard cover, 276 pages
Publisher InTech
Published online 16, May, 2012
Published in print edition May, 2012

This collection of books brings some of the latest developments in the field of watermarking. Researchers from varied background and expertise propose a remarkable collection of chapters to render this work an important piece of scientific research. The chapters deal with a gamut of fields where watermarking can be used to encode copyright information. The work also presents a wide array of algorithms ranging from intelligent bit replacement to more traditional methods like ICA. The current work is split into two books. Book one is more traditional in its approach dealing mostly with image watermarking applications. Book two deals with audio watermarking and describes an array of chapters on performance analysis of algorithms.

How to reference

In order to correctly reference this scholarly work, feel free to copy and paste the following:

Oleksandr V. Shishkin and Vitaliy M. Koshevyy (2012). Audio Watermarking for Automatic Identification of Radiotelephone Transmissions in VHF Maritime Communication, Watermarking - Volume 2, Dr. Mithun Das Gupta (Ed.), ISBN: 978-953-51-0619-7, InTech, Available from: http://www.intechopen.com/books/watermarking-volume-2/audio-watermarking-for-automatic-identification-of-radiotelephone-transmissions-in-vhf-maritime-comm

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821

© 2012 The Author(s). Licensee IntechOpen. This is an open access article distributed under the terms of the Creative Commons Attribution 3.0 License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

IntechOpen

IntechOpen