1H

UDC 621.326

Volodymyr Harbarchuk, Grzegorz Kozieł
Lublin University of Technology, Poland
wig@pluton.pol.lublin.pl

The Review of Sound-based Steganographic Techniques

The review of steganographic sound-based methods developed in the last ten years are presented in this article. The methods are grouped according to the domain of embedding the hidden information. The requirements introduced by phonographic industry were presented too.

Introduction

Steganography has been developing rapidly lately. It is particularly widely used in field of marking audio compositions. With dissemination of Internet access, illegal copying of audio compositions becomes more and more popular. This is considered as a serious problem for phonographic companies and for authors themselves, as they lose significant part of their royalties that way. Currently creating protection from data duplicating is not possible. It is necessary to mark the data in a way providing author with possibility of proving his authorship and other rights to the composition. Such marking should be done in such a way, that marked composition won't lose anything from its value – watermark must not introduce any audible distortions of a signal. Moreover, watermark's robustness to damage is a key matter. According to requirements introduced by International Federation of the Phonographic Industry (IFPI) [1], STEP2001 [2] and Secure Digital Music Initiative (SDMI) [3], watermark cannot be detectable by human senses (SNR, signal – noise ratio must be wider than 20 dB). Furthermore, reliable and unambiguous reading of watermark after time scale modification of ± 10 % must be possible. Added watermark has to outlast standard user-processing of audio material, such as MP3 compression, format change, low- and high-pass filtering. Majority of developed steganographic methods is used to composition watermarking. It is caused by huge demand from phonographic companies for such services. Majority of scientists try to meet all requirements of watermarking. Review of existing techniques and researches in the field of steganography of audio signals performed after 2000 year is presented in this article.

Amplitude modification

Amplitude modification method is known as least significant bit (LSB) method. It is well known and popular in communication as well as in watermarking [4]. Least significant bits of audio samples, which are not carrying valuable information but only quantization noise, are used for information concealment. Modifying the value of those bits do not affect on change of sound parameters and is usually inaudible for human ear. Unfortunately, this method shows no robustness to sound processing. Majority of popular modifications destroys carried information irretrievably. Information addition is usually carried by substituting least significant bits in all samples. It allows obtaining huge steganographic capacity coming to 1 kbps per 1 kHz of modified signal. However it may result in appearance of detectable noise, which may lead to easy reading of additional information.

Only some samples can be used to carry hidden information in attempt to avoiding such a situation. Appropriate algorithm, which should randomly choose points where additional data will be placed, considering sound parameters is order to obtain the best effects with the lowest possible signal distortions [4-6], should be used for its calculation.

Distortion interference may be minimized by matching appropriate carrier. For example noise caused by audience during concert recordings is a very good masker for additional data [1]. Shaping the characteristics of additional sequence in order to matching it with container signal is another possibility presented in [7]. It allows to reduce the level of entered distortion.

Low robustness to sound processing is the major flaw of methods based on amplitude modification. Usually simple format change destroys hidden information irretrievably. Error correction or hidden data duplication can be used for improving method's robustness, but it is preformed at the cost of steganographic capacity. In [5] authors proposed using LSB method in transform scope. First, transform is performed on container signal. Then additional data is attached to obtained coefficients using LSB method. Stegocontainer is received after performing reverse transform. Transforms: Fourier, cosine or continuous wavelet may be used in this method. This technique is also known as coefficient quantization.

Dither watermarking

Distortions are created during signal sampling. Dither is added in order to minimize them and to preserve as accurate signal waveform as it is possible. It is properly shaped low-power signal. Significant distortion elimination is possible at cost of addition small amount of noise. [1]. In order to add extra data to signal, Dither should be modified according to appropriate assumptions, and then original recording should be sampled [20]. This technique is known as quantization index modulation (QIM)[9]. In practice it is realized by using two different quantizers. Each one has to give out different values of result samples. Then value procured by first one will correspond with encoded value of 1, and value procured by the second one – with encoded value of 0 [9]. Fig. 1 presented in [9] illustrates how the method works. Points marked as X represents values procured by first quantizer and those marked with 0 are values procured by the second one. If bit of additional data has the value of 0, value represented by nearest X is treated as exit value. If value of 1 has to be encoded, value represented by nearest O is treated as an exit value. The distance d_{min} is the measure of method's robustness (the higher the distance, the more robust the method). Size of quantization cell is the measure of distortions introduced during the quantization process.

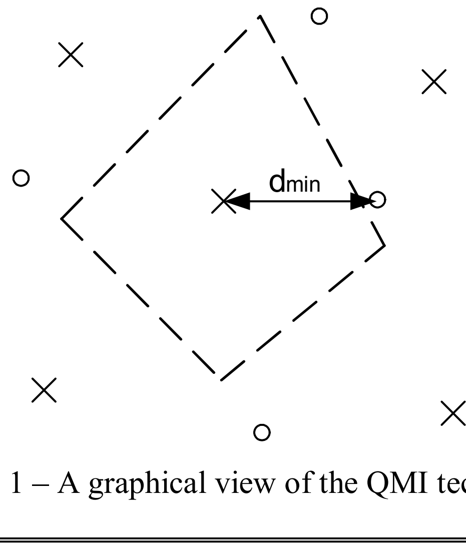

Figure 1 – A graphical view of the QMI technique

Echo watermarking

Human hearing is not able to detect the presence of signal echo, which appears during 2 ms period after the signal [10], if its amplitude does not exceed half of the signal's amplitude. This phenomenon can be used in order to hide additional information. Data concealment is performed by using steer able delaying filter, which is used to adding the copy of original signal delayed by set time to the signal itself, which is illustrated in fig. 2.

Figure 2 – Process of adding echo to the signal [11]

In order to obtain the possibility of symbol encoding, fixed echo delay values should be put down to each symbol, e.g. for value of 1 it can be the delay of 2 ms, and for value of 0 – delay of 1 ms (vide fig. 3) [6], [11]. In works [12], [13] perception conditions of additional echo signal are defined. Delay of 1 – 2 ms and amplitude not exceeding half of original signal amplitude are defined as border parameters. Encoding binary data in carrier required dividing it into blocks, in which independent echo shift by fixed value corresponding with value being encoded is realized. Creating two copies of the signal with added echo is the easiest way. Shift corresponding with binary value of 1 is used in the first one, while shift corresponding with binary value of 2 is used in the second. Subsequently both signals are divided into equal data blocks, which are received respectively from first or second signal and resulting in third one, which will be the carrier of hidden information. This process is illustrated in fig. 4. Delay change, which resulted in audible 'rattling' effect, turned out to be more problematic. Delay change of at most 0,05 ms with frequency not exceeding 10 ms should be used to avoid this problem. Satisfactory effects can be also obtained by smooth delay change.

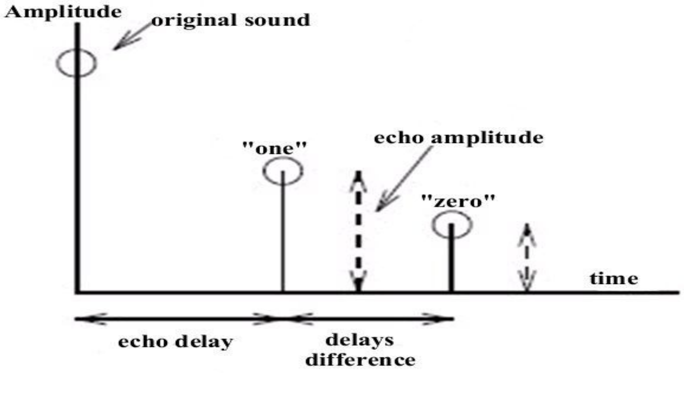

Figure 3 – Echo signals corresponding with logic values of 0 and 1 [11]

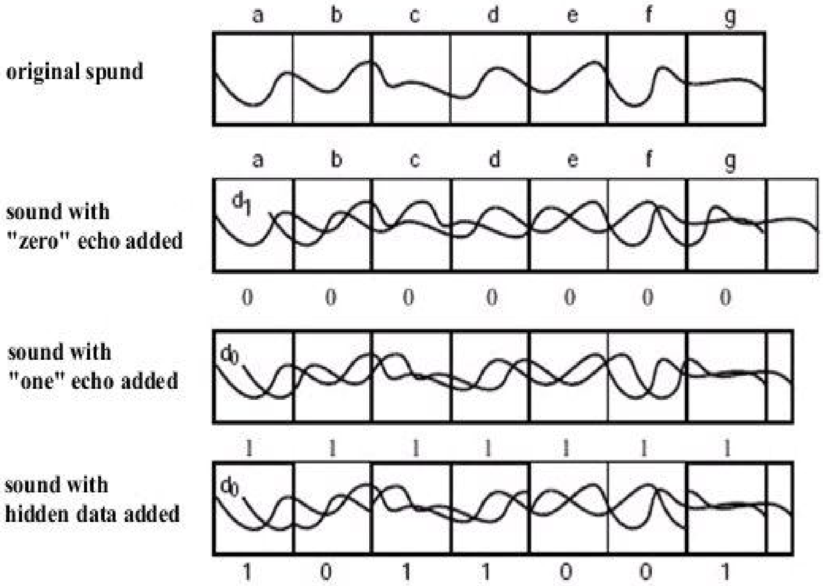

Figure 4 – Division of the signal into blocks and addition of the echo [11]

Hidden signal can be detected by computing the autocorelation of signal fragment with delays corresponding with logical values of 1 and 0. Results should be compared afterwards. The higher one points encoded value [14]. It is also possible to use amplitude characteristics of echo-setting filter. Spectrum of signal with hidden information should be logarithmized first, and then reverse discreet Fourier transform should be performed on it. As a result of those operations cepstrum of the signal is received, with stripes in places equal to k and to multiples of k, where k is the number of samples representing echo delay. Maximum value corresponds with echo delay being used and it allows reading of encoded value, both in this and previous method. Studies [12], [13] show beneficial influence of whitening signal spectrum on lowering error rate. Whitening is performed by using predict filter, which – after being adjusted to acoustic signal – periodically, every few dozen seconds transforms this signal into prediction error signal, which characterizes with lower autocorrelation and flattened spectrum.

Distance between signals encoding zeros and ones should be broaden in order to minimalize reading error rate. It is possible to using pre-echo (fig. 5a). It is echo signal added before actual sound. Then logic value of zero is encoded by adding echo before the signal, and logic value of one is encoded by adding echo after the signal. Phenomenon of lower signals being masked by higher ones following them is used here. It should be ensured that distance between signals and their values meet the masking conditions.

Some authors propose usage of polar echo (fig. 5b). It allows encoding data in other distance from signal than of echo. Encoding is performed by adding echo of different polarity. Positive polarity echo is used for encoding logic value of 1, while negative polarity echo is used for encoding logic value of 0. Using polar echo improves robustness of the method but it also introduces changes in timbre [4], [15-17]. In order to reduce this disadvantageous phenomenon authors [14] suggested using bipolar echo. Shapes of signals corresponding with encoded one and zero are shown in fig. 6. Such forming of additional signal minimizes timbre distortion by negative polarity echo significantly. Steganographical capacity of the method depends on size of the blocks into which signal will be divided (operations of adding fixed delay echo are performed on block of data), distance between blocks and data redundancy.

Subband filtration method with masking

Digital information can be also hidden by modifying signal cepstrum. Average values in certain ranges are changed or certain function is added to cepstrum value. Modification of cepstrum can also be treated as an operation supporting detection of signal echo, improving method's reliability. It consists in computing reverse discreet Fourier transform of logarithmized signal spectrum and using correlation of this spectrum and appropriate base functions (1) [11].

$$C(k_m) = \sum_{i=0}^{N-1} \hat{X}_i \exp(j2\pi k_m i / N), \tag{1}$$

where X_i is a sample of logarithmized spectrum of signal amplitude,

k_m – m-th coefficient of reverse discreet Fourier transform.

In order to increase correlation value $C(k_m)$, samples of logarithmized spectrum in i points should be increased when cos $(2\pi k_m i/N)>0$ and decreased when cos $(2\pi k_m i/N)<0$. Range of changes should not exceed masking threshold in order to avoid audible distortions. Masking threshold is computed on a principle used in MPEG-Audio coders. Only amplitude spectrum is modified. Phase spectrum is unchanging. Filtration is performed in subbands determined by sign of function cos $(2\pi k_m i/N)$, what is illustrated in fig. 5. Spectrum samples are increased by M_i, if they exceeded masking threshold or up to value of M_i, if they were below the threshold. Original phase spectrum should be added after modifying amplitude spectrum. Reverse Fourier transform should be performed afterwards.

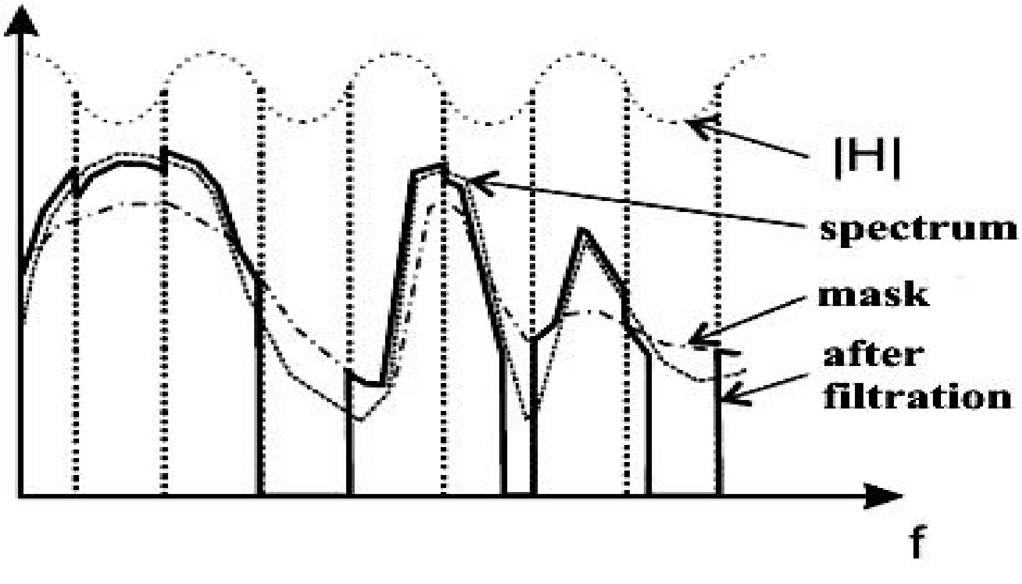

Figure 5 – Subband division and spectrum modification [11]

Research presented in [11] show: that described method of data concealment has very good results also as independent method, not accompanied by echo adding method.

Much lower power of transmission signal is an additional advantage of this method. On the other hand this method has a disadvantage of introducing audible distortions in form of "rattling". It is caused by step change of value of amplitude spectrum. In order to decrease this effect this method should not allow changes at the edges of data blocks. Changes should be made gradually inside the block until desired value is reached and smoothly return to the original state at the end of frame afterwards. To make that possible it is necessary to use the formula (2), which will be used to determine values of successive samples of modified signal.

$$x_n = \sum_{i=0}^{N-1} X_i(n) e^{j\phi_i} e^{j2\pi in/N} \qquad (2)$$

$X_i(n)$ changes within block limits from original value to target value and back. Distortions are practically eliminated while using blocks with size of 512 samples and passing times of 60 samples.

Spread spectrum methods

One of the main conditions of successful information concealment in a signal is its low power. Information dispersion in whole spectrum of used container signal allows unambiguous addition of data even if power of concealed signal is lower than power of noise [1]. Moreover information concealment in high-frequency bands has minimal influence on container signal. Using low-frequency bands allows high robustness. Information dispersion in all bands allows to gain compromise between robustness and invisibility. Information attached in that way introduces insignificant changes to the signal and is robust to damage and deletion, because it is hard to clean up the signal without damaging it significantly. Method of information dispersion in wide frequency band originates from telecommunication, where it is widely used in radio communication. Steganographical implementation bases on multiplying the signal of attached information with other, quasi-random signal with higher bit flow [5], [18]. This causes dispersion of signal spectrum, which is subsequently connected with container signal. Broadband signal is multiplied EX-OR in the container with identical quasi-random sequence, what results in spectrum compression and makes reading of the additional information possible. To read the information a key (used quasi-random sequence [3] is indispensable). To keep distortions at low level, watermark signal power should not exceed 0,5 % of container signal power [10]. Spread spectrum method is one of the better steganographic methods due to not only high robustness to detection, damage and deletion, but also to high steganographic capacity [1], [19]. It allows sending high-power signal, because it is dispersed on multiple frequencies. It allows obtaining small distance between signal and noise in every frequency range, what improves robustness to detection and damage of hidden information.

Phase coding

Human ear shows low sensitivity to sound phase change. This feature can be used for information concealment [4]. Method shown in [6] hides information in signal phase shifts. Concealment is performed by substituting signal fragments with the same fragments with shifted phase. Then each binary value is represented by different phase shift. It is done by dividing signal into fragments of fixed size. Next, Fourier transform is computed for each fragment. This results in creation of phase matrix. Phase matrix is changed in every fragment, that will be used as information carrier. Placing fragments with shifted phase next to each other would be disadvantageous regarding hearing sensitivity for relative phase shifts. That's why gaps, where phase matrix is modified in a way allowing signal phase continuity, are left between fragments. Knowledge of location and size of fragments being carriers of hidden information is essential for reading concealed data. This method allows gaining steganographic capacity of 32 bps.

Histogram techniques

Authors in [18], [20] suggest concealing information by modifying signal histogram. This method consists of 5 stages:

- From marked signal F, samples with amplitude in range $B=[-\lambda A, \lambda A]$ (λ – not negative, A – average value of amplitude module in recording) are chosen. On their basis histogram H_M illustrating numbers of samples with amplitude of a fixed value. Size of ranges M are selected so that their number is sufficient for watermark concealment.
- By qualifying samples to particular ranges portions marked as π are received. Afterwards samples inside each range are transformed by discreet continuous wavelet transform.
- Quasi-random sequence is created, which acts as watermark and is subsequently attached to the histogram.
- By using reverse continuous wavelet transform initial histogram is obtained. Next, it is disassembled in order to gain marked signal F'.
- Key is memorized in detector in order to further usage.

Watermark inserting begins with creating it by generating quasi-random sequence $W=\{w(i)|i=1,...,P\}$,which will be hidden in recoding F. Amplitude range ,which will act as a basis for creating histogram $B=[-\lambda A, \lambda A]$ is chosen afterwards. As during various signal transformations values of samples are changing, researchers should refer to average value of amplitude module of samples (3)

$$A = \frac{1}{N}\sum_{i=1}^{N} F(i). \tag{3}$$

Authors [20], [21] suggest, that best results can be obtained by using range λ *<0.5A, 2A>*. Three histogram ranges are required to encode one bit. Size of ranges should be chosen so, that their number would be sufficient for watermark insertion. If P is the size of additional data, number of histogram ranges L should not be lower than $3P$.

Encoding of single bit consists in appropriate change of proportions between number of samples in each range. If number of samples in ranges designed for encoding one bit as a, b and c, their sizes have to be modified according to formula (4) in order to conceal a single bit of data.

$$\boxed{\begin{cases} \dfrac{2b}{a+c} \geq T \; dla \;\; w(i) = 1 \\ \dfrac{a+c}{2b} \geq T \; dla \;\; w(i) = 0 \end{cases}}, \tag{4}$$

where T is a fixed threshold. Range size modification consists in change of amplitude of samples, so that they will land in next histogram range. This operation is always performed simultaneously on three histogram fragments, which will store one bit of information. To obtain transformation robust to TSM and mp3 compression threshold T should be set to value higher than 1,1. In practice, authors [20], [21] present results for T=1,4, λ*=2,4* and P=40, moreover they assume the possibility of correct watermark identification with 15 % reading error rate. Using those values of coefficients allow obtaining TSM robustness in range from –10 % to +10 %, change of sampling frequency, low-pass filtration, noise addition, random insertion of small signal fragments, volume change in range from –20 % to +20 %, loss compression and jitter effect.

Using significant signal fragments

The time scale modifications are relatively big threat for all steganographic techniques. There are very few methods, which are able to attach information in a way allowing it to outlast extending or reducing the recording by few per cent. Human hearing is not very sensitive to TSM, so additional information can be deleted easily. Currently used TSM algorithms are designed to preserve the highest quality of scaled sound. It is possible by diverting operations performed on individual signal fragments, for sound is not "stretched" regularly. First it is analyzed in order to determine fragments, which human hearing is particularly sensitive to. Those fragments are modified very slightly or not at all. The rest of signal are modified in a way, which allows achieving desired length of whole composition. Lee and Xue in [22] noticed, that this makes inserting watermark robust to TSM possible. They also proposed using composition segments not modified during TSM for information concealment. In order to detect those regions pass capacity signal filtering should be performed, leaving d3 band (with range 3kHz – 5 kHz). This is the range of frequencies, which are well audible by human ear, thus not modified by TSM algorithms. Besides, sound generated by majority of instruments include this component. Example recording with visible d3 band is shown in fig. 1. Maxima found in analyzed subband show places, which are slightly modified during TSM. Lee and Xue proposed using this places for watermark inserting. Watermark inserting procedure consists of five phases:

- continuous wavelet decomposition of original signal in order to separate d3 band;
- flattening d3 band by noise reduction – emphasizing the maximums;
- local maximum (LM_i) detection and determining places of its occurrence;
- determining areas *R,* to which watermark will be attached according to formula

$$R=\{R_i|\ R_{i=}\ LMi–F_{Length}/4:\ L_{Mi}+F_{Lengt}h*3/4–1\}, \qquad (5)$$

where F_{Length} is the size of attaching area (Lee and Xue show results for area of size of 4096 samples);

- adding watermark to each of determined areas.

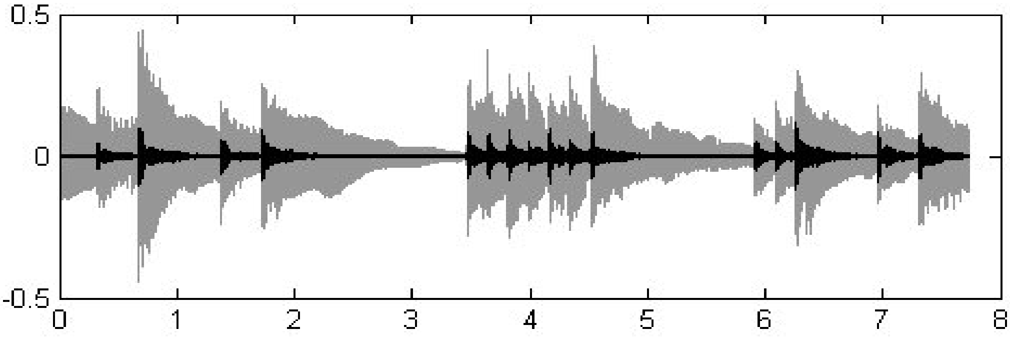

Figure 6 – Audio signal (gray) with visible d3 band (black) [22]

Maximum size of added sequence, not causing audible interferences, is determined as 64 bits for area of size of 4096 samples. It is quasi-random binary data sequence *W* (6). Before addition it is modified by BPSK algorithm, according to formula (7), which changes values {0,1} to {–1,1}, resulting in sequence *W'*.

$$W=\{w(i)|w(i)\in\{1,0\},\ 1\le i\le 64\}, \qquad (6)$$

$$W'=\{w'(i)|w'(i)=1–2*w(i),\ w'(i)\ \in\{+1,–1\},\ 1\le i\le 64\}. \qquad (7)$$

Afterwards, successive bits *W'* are added to attachment area by changing coefficients of performed Fourier transform according to (8).

```
for l=1:LF
    for k=1:64
        flag=RF(off+2*k-1)<RF(off+2*k)                                   (8)
        if w'(k)= =1 end flag= = 1 change value
        if w'(k)= =-1 end flag= = 0 change value
    end,
```

where *RF(off+2*k–1) and RF(off+2*k)* are the coefficients of Fourier transform in frequency band of 1 kHz to 6 kHz, *off* is user-established shift. Reverse Fourier transform is used for return into the time realm. Signal watermarked by described method and introduced interferences are shown in fig. 7.

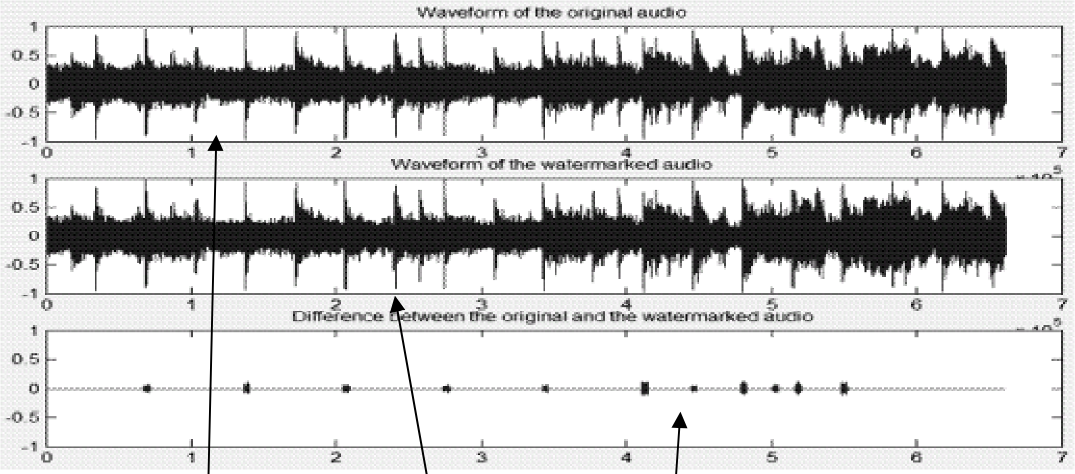

Figure 7 – (a) original signal, (b) marked signal, (c) signal difference [22]

Tests carried out by authors of the algorithm showed, that it is immune to mp3 compression with output of 32 kb/s, low-pass filtering, noise addition, sampling frequency change, echo addition, random insertion of signal fragments with size not exceeding 10000 samples, noise reduction and TSM up to 16 %. In [23] authors suggest similar method of watermark insertion, where edges of signal or local maximums of signal energy are the attachment areas.

Modification of distance between significant signal points

Mansour and Tewfik in [24] suggest adding information to audio signal by modifying distance between significant signal points. Location of this points is determined by continuous wavelet transform. Local extremes of wavelet coefficients show location of minima and maxima of signal derivative – they show location of the edges of signal. Edge of signal is a passage from silence to sound and location of basic frequency change. Suggested algorithm is based on idea of modification of distance between maxima of wavelet coefficients. Algorithm scheme is shown in fig. 8.

Algorithm operates in five steps:

1. Computing signal envelope by low-pass filtration.
2. Performing nonorthogonal wavelet decomposition of envelope, which coefficients *C(τ)* will be used in further steps.

3. Minimizing power of vector of coefficients and locating local maximums in it.
4. Thresholding extremes in order to leave only the highest.
5. Modifying distance between selected extremes in order to conceal information.

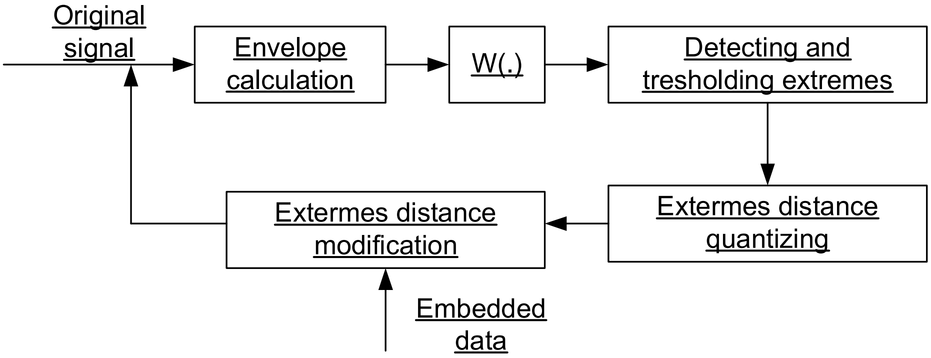
Original signal
Envelope calculation
W(.)
Detecting and tresholding extremes
Extermes distance quantizing
Extermes distance modification
Embedded data

Figure 8 – Scheme of algorithm

The authors of this algorithm also base on operating principle of TSM algorithms, which slightly modify significant fragments of signal. Fragments of signal detected by wavelet decomposition are analyzed in order to determine the importance of detected change. Only most significant edges, which will not be modified during signal transformation, are used for information concealment. Distance between individual maxima are quantized by determining distance ranges which are equivalent to binary values of zero and one. Afterwards they are modified according to sequence of attached data, so that each of distances between analyzed maxima will be located in central part of range. It will allow to obtain higher robustness to time scale modifications, which can extend or shorten the recording irregularly. Tests carried out by creators of the algorithm showed, that it is robust to mp3 compression with capacity of 32 kb/s, low-pass filtering, change of sampling frequency, noise reduction and TSM up to 10 %.

Methods operating in the transform domain

Transform methods are based on converting traditional signal recording in frequency domain. This signal representation is called wavy or spectral. Signal recording conversion is performed by using appropriate transform. Data concealment is done by modifying received transform coefficients, which are afterwards subjected to reverse transform [1]. Transform methods show high robustness to signal compression. Unfortunately, they are not robust for time scale modifications. Authors [25] present method robust for resynchronization caused by random cropping and increased robustness for compression. Algorithm divides container signal into segments. Each segment is divided into two parts. First part is used for adding synchronization code, which allows to identify the location of information attachment. Barker code is used for this purpose. Second part of segment is used for attaching the information. The procedure is performed in two stages to increase robustness. First, continuous wavelet transform is performed on processing fragment. Second, cosine transform is performed on resulted low frequency coefficients. Information is hidden in coefficients of this cosine transform.

Summary

Steganography is a branch of science, which is currently developing very rapidly. Information concealment in sound is particularly popular because of huge demand from phonographic industry for watermark techniques. Majority of authors focus on obtaining high robustness of additional data for common operations with preserving acceptable signal to noise ratio. There is no ideal method, which will be robust to all transformations. Every method has its own, different advantages. Unequivocal comparison of all methods is very difficult, since each author gives out results in a different way, exposing advantages of his own method.

Literature

1. Katzenbeisser S., Petitcolas F. A. P. Information Hiding Techniques for Steganography and Digital Watermarking. – London, 2000.
2. Режим доступа: www.trl.ibm.com/projects/RightsManagement/datahiding/dhstep_e.htm.
3. SDMI Call For Proposals, Phase II, 2000. – [Электронный ресурс]. – Режим доступа: http://www.sdmi.org/download/.
4. Bassia P., Pitas I. Robust audio watermarking in the time domain. – 1998.
5. Dugelay J. L., Roche S. A survey of current watermarking techniques. – Information hiding: Techniques for steganography and digital watermarking. – Boston, 2000. – P. 212-148.
6. Johnson N.F., Katzenbeisser S.C. A survey of steganographic techniques, Information hiding: Techniques for steganography and digital watermarking. – Boston, 2000. – P. 43-48
7. Czerwinski S., Fromm R. Digital music distributionand audio watermarking. – Berkeley, 1999.
8. RLE Massachusetts, 1999. – [Электронный ресурс]. – Режим доступа: http://rleweb.mit.edu/Publications/currents/cur111/11-1watermark.htm
9. Chen B., Wornell G.W. Quantization index modulation: A class of provably dood methods for digital watermarking and information embedding. – Sorrento, 2000.
10. Bender W., Gruhl D., Morimoto N., Lu N. Techniques for data hiding // IBM system Journal. – 1996. – № 5.
11. Dymarski P. Filtracja sygnałów dźwiękowych jako metoda znakowania wodnego i steganografii. – Bydgoszcz, 2006.
12. Dymarski P., Pobłocki A., Baras C., Moreau N. Algorytmy znakowania wodnego sygnałów dźwiękowych. – Krajowe Sympozjum Telekomunikacji. – Bydgoszcz. – 2003.
13. Pobłocki A. Cyfrowe znakowanie wodne sygnałów dźwiękowych z wykorzystaniem echa. – Praca dyplomowa. – 2003.
14. Режим доступа: http://pl.wikipedia.org/
15. Gruhl D., Lu A. Echo Hiding. Information Hiding Workshop. – Cambridge University(U.K.). – 1996. – P. 295-315.
16. Garay A. Measuring and evaluating digital watermarks in audio files. – Washington. – 2002.
17. Kim S., Kwon H., Bae K. Modification of Polar Echo Kernel for Performance Improvement of Audio Watermarking. – Berlin, 2004.
18. Kirovski D., Malvar H. Robust cover communication over a public audio channel using spread spectrum. – Pittsburgh, 2001.
19. Tomaszewski M. Analiza algorytmów steganograficznych.
20. Xiang S., Huang J., Yang R. Time-Scale Invariant Audio Watermarking Based on the Statistical Features in Time Domain // Artificial Intelligence and Lecture Notes in Bioinformatics. – 2007. – P. 93-108.
21. Xiang S., Kim H., Huang J. Audio watermarking robust against time-scale modification and MP3 compression. – [Электронный ресурс]. – Режим доступа: http://ieeexplore.ieee.org
22. Li W., Xue X. Audio Watermarking Based on Music Content Analysis: Robust against Time Scale Modification. – Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). – 2004. – P. 289-300.
23. Li W., Xue X., Lu P. Localized audio watermarking technique robust against time-scale modification // IEEE Transactions. – 2006. – Vol. 8, Issue 1. – P. 60-69.
24. Mansour M., Tewfik A. Audio Watermarking by Time-Scale Modification // Proc. IEEE 3 International Conf. on Acoustics, Speech and Signal Processing. – P. 1353-1356.
25. Wang X., Zhao H. A Novel Synchronization Invariant Audio Watermarking Scheme Based on DWT and DCT // IEEE Transactions on signal processing. – 2006. – Vol. 54.
26. Bogumił D. Cyfrowe znaki wodne odporne na kompresję. – JPEG. – Warszawa, 2001.
27. Garbarczuk W., Świć A. Podstawy ochrony informacji. – Politechnika Lubelska Lublin, 2005.

В. Гарбарчук, Г. Козел

Запропоновано оглядовий аналіз найважливіших напрямків досліджень в стеганографії за остатні 10 років з систематизацією методів за способом приховування інформації в звукових контейнерах та врахуванням розвитку акустичної техніки.

Статья поступила в редакцию 17.07.2008.