UDC 681.3

Volodymyr Harbarchuk, Grzegorz Koziel
Lublin University of Technology, Poland
wig@cs.pollub.pl

Properties of a New Fourier Transform-based Steganographic Method

A new Fourier transform-based steganographic method is proposed. The practical verification of properties of the presented algorithm is analyzed and discussed. The analysis of algorithm robustness to the damage of the hidden information is also conducted.

Introduction

Fourier transform has not gained popularity in audio signal steganography due to problems with obtaining stegocontainers which do not contain audible distortions. The human auditory system is very sensitive to changes of the sound frequency. The modification usually introduces distortions clearly audible by humans. Creating stegocontainer with inaudible distortions to the human is only possible by using a masking. This fact was used in the presented method to create stegocontainers.

Masking

Masking is the phenomenon which causes that the human auditory system is not able to record some sounds (masked) because they are "overwhelmed by other sounds (masking sounds)" [1]. Two types of masking can be distingiushed:

- insimultaneous,
- simultaneous.

Insimultaneus masking (temporary) is based on blocking the perception of the signal followed by a loud signal at the time interval of less than 40 ms after masked sound or up to 200 ms before it. This applies to mask sounds quieter than the masker. The appearance of a louder sound can be noticed at any time.

Frequency masking (simultaneous) is based on masking the quieter sound by sound louder at the same time with a similar frequency. Masking condition is that the masked sound was below the masking threshold. Masking threshold value depends on the frequency and nature of the masked and masking tone (whether it is a pure tone or narrowband noise). This dependence of a masking changes signal with a frequency of 1 kHz is shown in Figure 1.

Masking noise is much more difficult, because human ear is particularly sensitive to the presence of this type of interference. Thus, the audibility threshold in the case of masking noise with pure tone will be much lower than that of the pure tone masking the noise. The distance between the masking and masked signal is denoted by the symbol SMR (*Signal Mask Ratio*). It has a maximum value on the left border of the *critical bandwidth* which contains the elementary frequency bandwidth of the acoustic power equal to acoustic power of the simple tone of frequency placed in the middle of that bandwidth, while discussed simple tone has the intensity, that it is on the border of audibility while being overwhelmed by unlimited bandwidth of continuous noise. Inside this band, the noise caused by attaching the information is heard while the distance signal to noise ratio SNR is greater than the SMR.

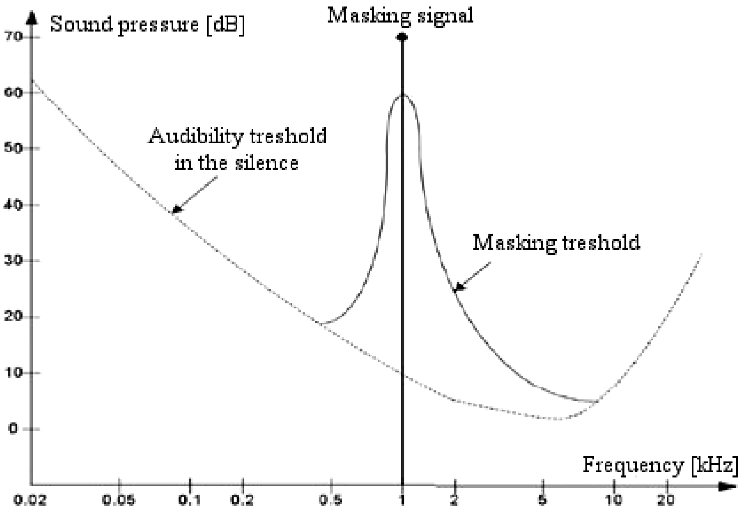

Figure 1 – Simultaneous masking threshold for 1 kHz sinusoidal masking signal while masking the “pure” sound [2]

If assumed, that all distortions are caused by attaching additional data, and the SNR(m) denotes the distortion of the m-th critical band, then the audible distortions may be defined as the distance between the noise and the threshold of audibility of the distortion of NMR calculated by the formula:

$$\mathrm{NMR}(m) = \mathrm{SMR} - \mathrm{SNR}(m) \tag{1}$$

The variability of the SMR and SNR in the frequency domain is presented in Fig. 2.

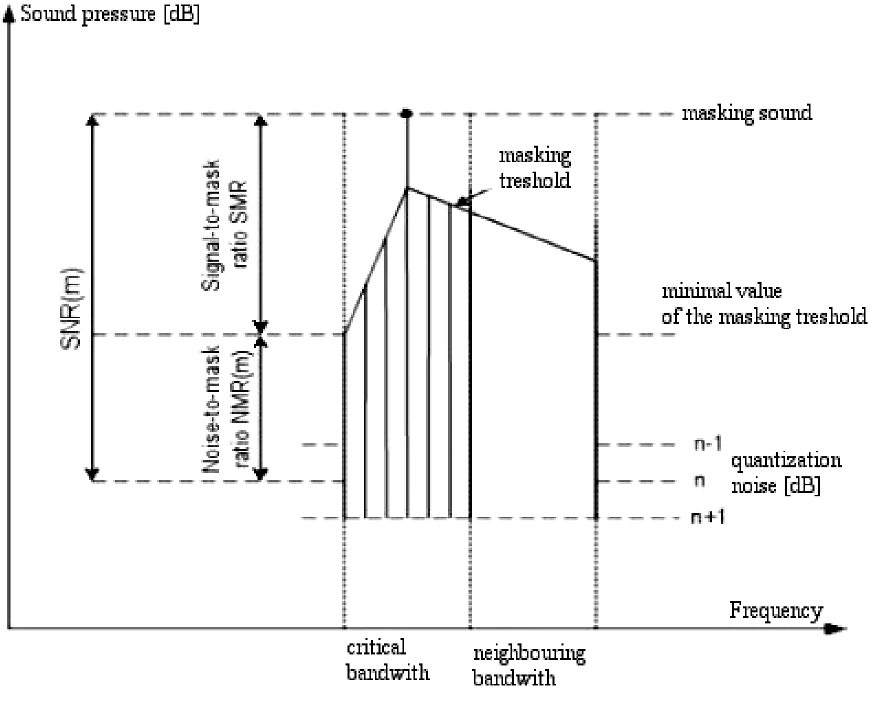

Figure 2 – SMR and SNR values [2]

While analyzing the properties of masking it was noted that the use of insimultaneous masking does not allow the use of all parts of the signal to hide the additional information and is also problematic in implementation if modifications to the analyzed signal are introduced at the same time. It is possible to obtain much better results by using simultaneous masking, which allows using all parts of the signal for the purpose of steganography. Therefore, this type of mask was chosen to conceal the changes in the signal of stego-container introduced by the algorithm. It is possible here to use existing masking models implemented in many audio compression algorithms. However, it is important to realize that the masking model is used to assess the compression algorithm, which sounds are not relevant to the sound quality and then to remove them from the signal.

Using the same masking model would led to the creation of stegocontainer without audible distortions, but it would also negatively influence the robustness of hidden data, which would be removed or at least substantially damaged by compression.

To preserve the robustness of attached information while masking the amine introduced by hiding the information at the same time, it was necessary to develop an independent masking model. The research showed that it is possible to obtain very good results by using a simplified masking model described by the equation of the second degree of the form:

$$W_g = (a - (f_{\max} - f)^2 / b) \cdot W_{\max} \, , \qquad (2)$$

where *a, b* – coefficients of the equation taken from steganographic key, *f* – frequency, f_{max} – masker frequency, W_{max} – masker amplitude, W_g – allowable amplitude of masked stripe.

A sample curve described by the equation 2 is illustrated in Figure 3. This curve was created after substituting the value of a = 0,6 and b = 30000 into equation 2.

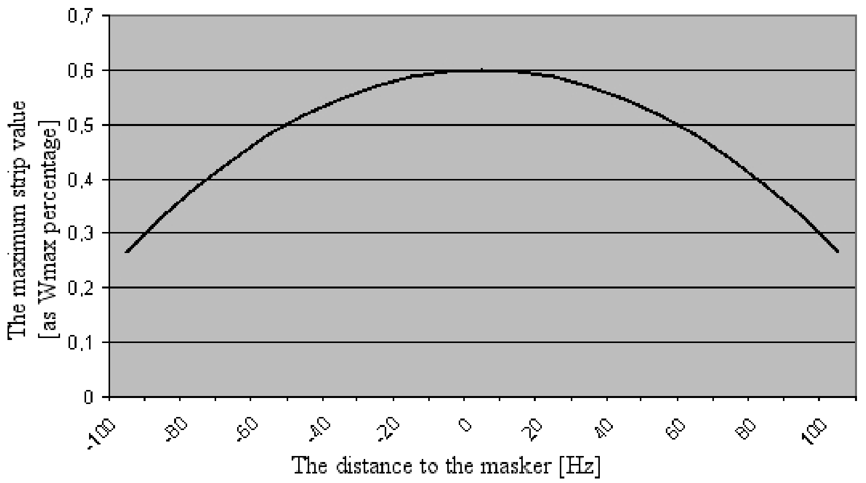

Figure 3 – Curve approximating the course of masking threshold [own work]

The curve presented in Figure 3 sets the masking threshold, below which the changes made to the signal are inaudible. In the developed algorithm the presented curve determines the maximum value of the modified sound frequencies and influences the choice of the used frequency bands used. It is an additional advantage, because without knowledge of its course the person trying to read the attached message is not able to determine which bands of spectrum were used to hide the additional information.

The exact theoretical basis of the presented methods were presented in the author's own papers [3], [4].

The correctness of the proposed masking model and selection of *a* and *b* coefficients was confirmed in a double blind listening test. Five-step marking scale was used:

1 – no differences,

2 – not sure,

3 – very weak interference,
4 – weak interference,
5 – clearly audible distortion.

In order to determine the reliability of the test, two sets of original recordings were used. The obtained results were marked as a comparison with the signal modified with the strength of 0 %. The results of the test are presented in Figure 4.

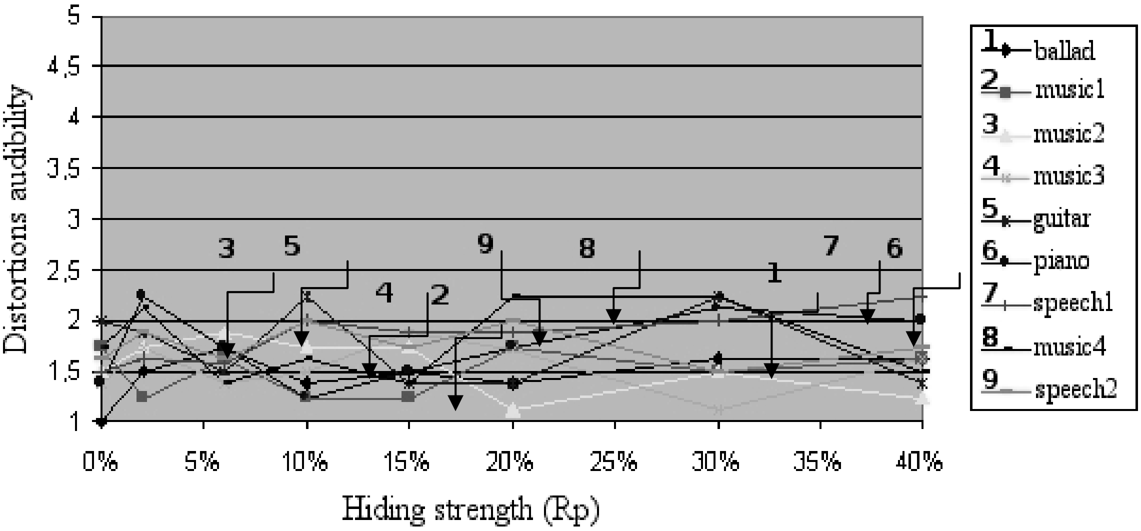

Figure 4 – Interferences audibility in the function of the hiding strength [own work]

As shown in the graph shown in Figure 4 testers failed to clearly identify the tracks containing the attached data. The results obtained for the modified recordings are similar to results obtained while comparing two identical signals. In some cases, the original recording was marked as being more “suspect” than the modified one. In addition, extreme values only slightly exceed the value of 2, which means the uncertainty of the existence or absence of additional signal in the test. It can be concluded that the method developed in the tested range does not introduce audible distortion to the average listener, which allows the use of $R_p \leq 40$ %, where R_p means the strength (value) of the modification and is defined as the ratio of the masker value W_{max}.

Distortions introduced by the method

Attaching additional data always creates changes in the original signal. However, these changes may not be too large, as this would suggest the existence of internal information and could serve as guidance to stegoanalytic. To determine the size of entered distortions, the objective measures described in [5-7] were used:

- Mean square error (MSE),
- Normalized mean square error (NMSE),
- Signal to noise ratio (SNR),
- Peak signal to noise ratio (PSNR),
- LP standard (LP),
- Maximum difference between the original and modified signal (MD),
- Average absolute difference between the signals (AD),
- Normalized average absolute difference between the signals (NAD),
- Hidden data transparency (AF).

Due to the dependence of the obtained values from attaching force R_p, the distortion levels introduced by various forces while including additional information are presented in Table 1.

Table 1 – Distortion introduced by presented method [own work]

Rp, %	MSE	NMSE	SNR [dB]	PSNR [dB]	LP	MD	AD	NAD	AF
1	7E-6	1,3E-3	29,0	99,9	7 E-6	0,06	1E-3	0,02	1
10	9E-6	1,7E-3	27,6	98,5	9 E-6	0,06	1,6E-3	0,03	1
15	1,4E-5	2,7E-3	25,7	96,6	1,4E-5	0,06	2E-3	0,04	1
20	2,3E-5	4,3E-3	23,6	94,5	2,3E-5	0,06	2,8E-3	0,06	1
30	5,6E-5	1E-3	19,8	90,7	5,6E-5	0,06	4,3E-3	0,09	0,99
40	1E-4	2E-3	17,0	87,9	1E-4	0,08	5,8E-3	0,12	0,98

The presented measurements show that the level of generated distortions is low enough for the changes not to be noticed. This is confirmed by listening tests which results are presented in Fig. 4.

Filtering robustness

Filtering is an operation often performed on acoustic signals in order to remove unwanted frequency components. Robustness to such operations is desired. In order to evaluate the robustness to filtration of the developed algorithm, an experiment was carried out in which the stegocontainer was subjected to bandpass filtering. The obtained results are presented in Table 2.

Table 2 – The filtering robustness of the presented method

Sound	Number of erroneously read bits, %				
Bandwidth throughput	20Hz –22kHz	60Hz –22kHz	100Hz – 22kHz	200Hz – 22kHz	1kHz –22kHz
Piano	0,7	2,8	2,8	8,6	42,1
Trumpet	3,6	4,5	5,0	5,0	21,8
Speech	10,0	16,0	20,6	33,3	48,7
Music	9,3	8,3	11,8	15,3	49,3
Bandwidth throughput	20Hz –22kHz	60Hz –22kHz	100Hz – 22kHz	200Hz – 22kHz	1kHz –22kHz
Piano	0,7	2,8	2,8	8,6	42,1
Trumpet	3,6	4,5	5,0	5,0	21,8
Speech	10,0	16,0	20,6	33,3	48,7
Music	9,3	8,3	11,8	15,3	49,3

The sensitivity to filtering out a specific frequency band cannot be clearly defined in case of the presented method. This sensitivity will be different for each signal. This is caused by a completely different distribution of data in each signal depending on its parameters.

While analyzing the obtained results it can be seen that the increase in the number of incorrectly read bits is closely related to filtering out a wider range of audible frequencies.

This is consistent with the principle of the method – hiding data in the audible frequency range near the frequency of the highest energy. However, the obtained results allow to conclude that it is impossible to damage the hidden data without causing significant damage to the signal of the stegocontainer.

Analysis of the noise impact on damaging the attached data

There are many sources that generate noise, to which the signal is exposed. They make changes to the signal, which often take the form of audible distortions. In addition, they modify the parameters of a stegocontainer damaging the contained information. In order to determine the robustness of the presented method to noising the stegocontainer, an experiment was conducted – white noise of a certain strength was introduced to the stegocontainer. The obtained results are presented in Figure 5.

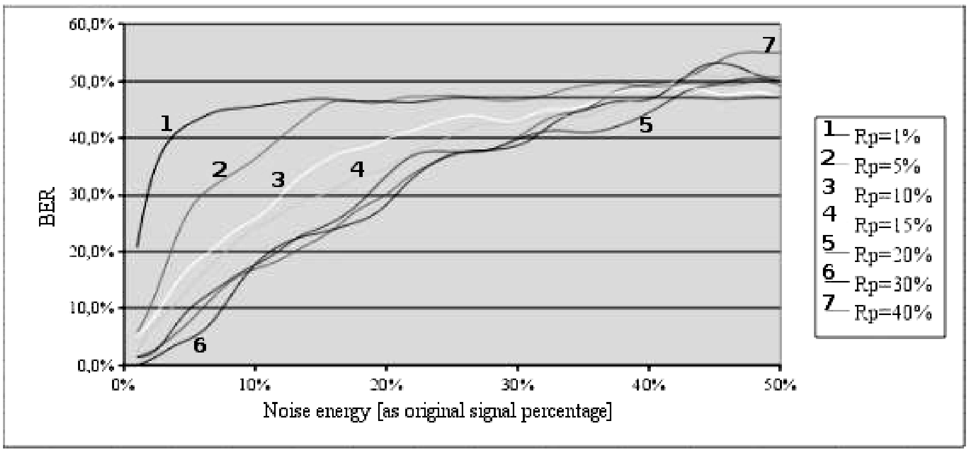

Figure 5 – Presented method resistance to noise adding [own work]

While analyzing Figure 5 it can be noticed, that with increasing noise strength, the number of reading errors also increases. Moreover, correlation between robustness to noise attachement and applied join force R_p appears.

Increased value of R_p results in greater differences in values between the spectrum strips. Damaging the attached information requires using changes with greater power. Obtained results are consistent with the theoretical assumptions of the method.

Evaluation of robustness to the dynamic transformation

Any transformation that changes the signal amplitude is called a dynamic transformation. In order to assess the impact of this kind of modification on the bit error rate, the prepared stegocontainers were subjected to modification like silencing signal and standardization combined with removal of DC. The obtained results are presented in Table 3.

Table 3 – Robustness of presented method to dynamic transformation (the table shows the BER value) [own work]

silencing, %				standardization, %			
music	speech	piano	trumpet	music	speech	piano	trumpet
4,4	4,6	2,1	1,3	4,4	5,3	2,1	0

Results show a high robustness of data hidden by using the developed method to the dynamic transformations. It is possible due to the fact, that the presented method calculates the target values of the modified stripes basing on key and masker value independently in each signal fragment.

If small fragments are used, changes made within the portion treated can be treated as equal for all samples. The proportions between the different samples stay similar to the original and only minimally affect the changes of signal spectrum. Due to this fact the presented method is able to adapt to changes in the dynamics of the signal, resulting in a high resistance to dynamic transformation.

Analysis of susceptibility to damage by operations influencing the spatial effect

Sometimes, in order to obtain richer sound, echoes signal is added to the sound signal. It is also used in the watermarking the recordings.

Due to its high popularity, this operation was used to assess the vulnerability of hidden data to transformations influencing the spatial effect. For stegocontainers which were prepared by the presented method, an echo signal was added, with a force of 10 % of the original signal, 2 ms delay to the original. Then there was an attempt to read the attached information from the prepared media. The obtained results are shown in Table 4.

Table 4 – Robustness of compared methods to operations influencing the spatial effect [own work]

method	music	speech	piano	trumpet
MF, %	7,9	13,3	4,3	10,0

The method shows a high level of robustness to the echo attaching operation, despite the fact that data is hidden in the audible band. This is possible due to the adjustment of join forces to the energy of the signal.

Robustness to format change and compression

In case when change of the media format during the transmission of data from sender to recipient is possible, it is necessary to provide robustness to transformation, which the media may be subjected to.

Many steganographic methods do not provide robustness or provide it on a very low level. Evaluation of compression robustness was done by converting stegocontainer to a specific format and then re-converting it into an original format. Then, the information was read from the stegocontainer. By comparing it with the original version, the number of incorrectly read bits was determined. Results of the tests determining robustness to various compression formats are presented in Figures 6 – 9.

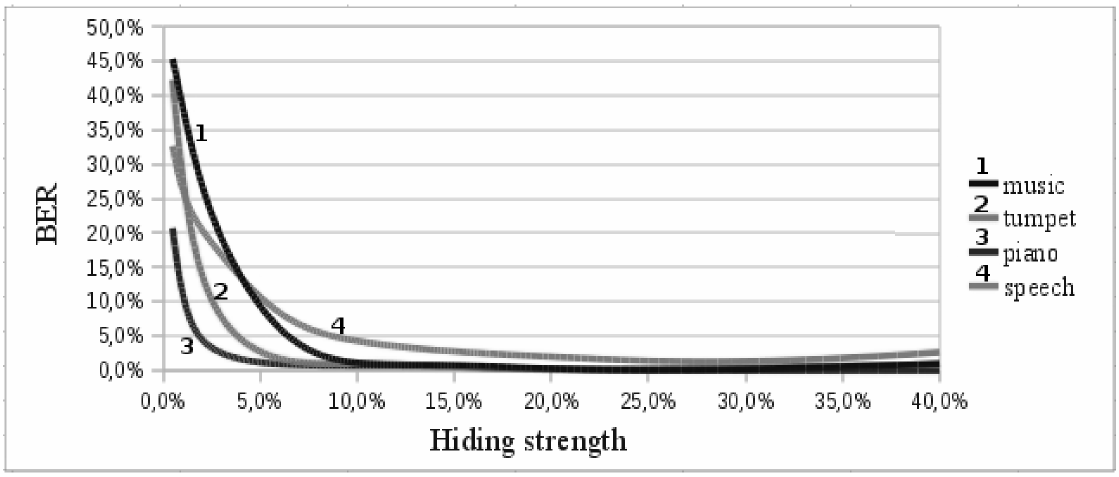

Figure 6 – The MP3 128 kbit/s compression resistance

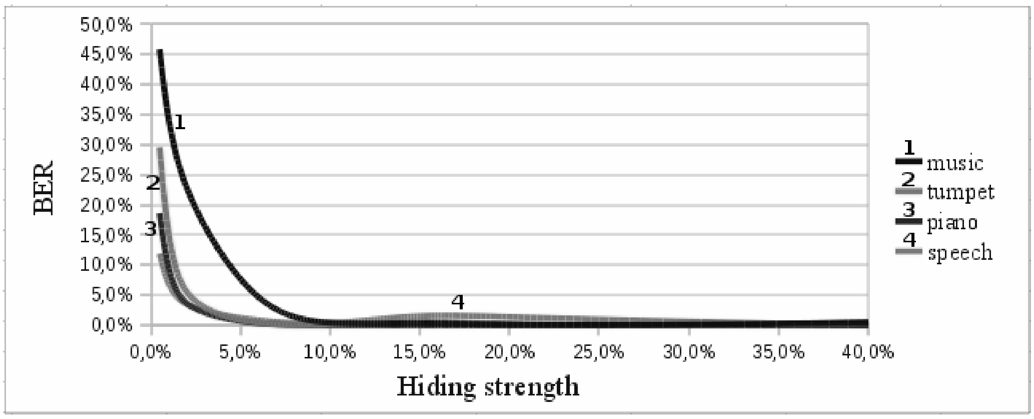

Figure 7 – The OGG 128 kbit/s compression resistance

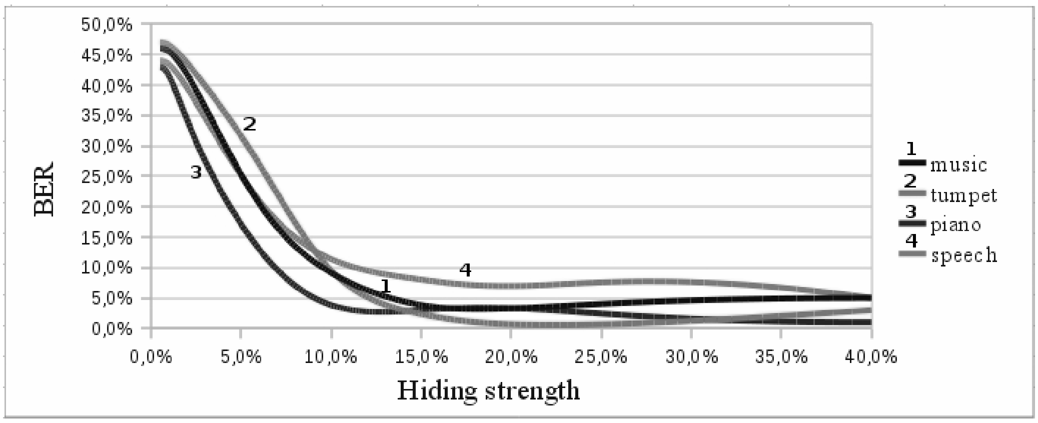

Figure 8 – The AAC 128 kbit/s compression resistance

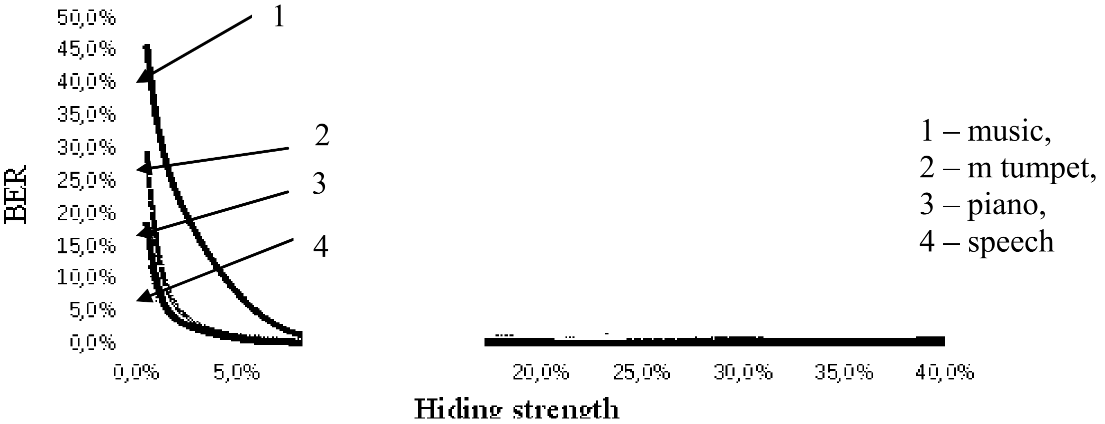

Figure 9 – The WMA 128kbit/s compression resistance

The research showed that while using a sufficiently large value of hiding strength, the described method shows good robustness to the tested types of compression. Moreover, the dependence of robustness to the value of hiding force is similar for all tested formats.

Conclusion

Applying the proposed method allows to obtain the stegocontainer characterized with high robustness to damage to the hidden information as a result of various transformations of the stegocontainer. Due to attaching the information to the audible band of frequencies and to its dispersion across the wide frequency range of this band, damaging the hidden data is impossible without introducing audible distortions to the signal. Furthermore, the removal of certain frequency ranges indicates that the attack on the stegocontainer was carried out.

The size of the value changes of spectral stripes depends on the value of the largest stripe in the spectrum acting as masker. This allows to obtain an optimal solution for both robustness and adaptation of ongoing changes in the amplitude of the signal in the selected part of this signal and to use all the fragments to hide the additional information, regardless of their volume.

Literature

1. Johnston J. Wideband coding perceptual considerations for speech and music, Advances in Speech Signal Processing / J. Johnston, K. Brandenburg. – 1992. – P. 109-148.
2. Cvejic N. Algorithms for audio watermarking and steganography / N. Cvejic. – Oulu University Press 2004.
3. Kozieł G. Method of concealing information in sound based on Fourier transform and masking / G. Kozieł // Polish Journal of Environmental Studies. – 2009. – P. 181-186.
4. Kozieł G. Fourier transform and masking in sound steganography / G. Kozieł // Актуальні Проблеми Економіки. – 2009. – № 12. – 2009.
5. Garay A. Measuring and evaluating digital watermarks in audio files / A. Garay. – Master thesis, 2002.
6. Mahbour R. Multimedia Technologies: concepts, methodologies, tools, and applications / R. Mahbour, M. Syed – London, 2008.
7. [Электронный ресурс]. – Режим доступа: http://pl.wikipedia.org/wiki/Bit_Error_Rate.

В. Гарбарчук, Г. Козел

Свойства нового стенографического метода на основе модификации преобразования Фурье

Предложен новый стеганографический метод на основе модификации преобразования Фурье. Практическая реализация и тестирование алгоритмов на основе этого метода показали его высокую эффективность.

В. Гарбарчук, Г. Козел

Властивості нового стенографічного методу на основі модифікації перетворення Фур'є

Запропоновано новий стеганографічний метод на основі модифікації перетворення Фур'є. Практична реалізація і тестування алгоритмів на основі цього методу показали його високу ефективність.

Статья поступила в редакцию 24.06.2010.