Grzegorz Koziel[1]

INCREASING STEGANOGRAPHIC CAPACITY OF THE MF METHOD

The MF method was developed by the author. It has a good robustness against compression, filtration and other common operations. The problem is in small steganographic capacity. The article presents a way of steganographic capacity increase in this method. It is possible due to bigger number of local maxima usage. The MF method uses only one global maximum of sound spectrum. In its modified version local maxima are used too. Each maximum is used to hide a separate bit of additional information. It allows obtaining greater steganographic capacity.

Keywords: *steganography, information hiding, Fourier transform.*

Гжегож Козел

ПОКРАЩЕННЯ СТЕГАНОГРАФІЧНИХ ВЛАСТИВОСТЕЙ МОДИФІКОВАНОГО МЕТОДУ ФУР'Є

У статті описано модифікований метод Фур'є, розроблений автором. Метод має досить непогані показники компресії, фільтрації та інші загальні параметри, недоліком методу є його незначна стеганографічна здатність. Представлено спосіб підвищити даний показник шляхом збільшення числа локальних максимумів. У першій модифікації методу використовується один глобальний максимум звукового спектру. В оновленій версії методу також використовуються локальні максимуми. Кожен з максимумів використовується для приховування окремого біту додаткової інформації. Це й дозволяє покращити стеганографічні якості методу.

Ключові слова: *стеганографія; приховування інформації; перетворення Фур'є.*

Форм. 4. Рис. 2. Літ. 9.

Гжегож Козел

УЛУЧШЕНИЕ СТЕГАНОГРАФИЧЕСКИХ КАЧЕСТВ МОДИФИЦИРОВАННОГО МЕТОДА ФУРЬЕ

В статье описан модифицированный метод Фурье, разработанный автором. У метода довольно хорошие показатели по компрессии, фильтрации и другим общим параметрам, недостатком же является его малая стеганографическая способность. Представлен способ повысить данный показатель путем увеличения числа локальных максимумов. В модификации метода используется один глобальный максимум звукового спектра. В обновленной версии метода также используются локальные максимумы. Каждый из максимумов используется для сокрытия отдельного бита дополнительной информации. Это и позволяет улучшить стеганографические качества метода.

Ключевые слова: *стеганография; сокрытие информации; преобразования Фурье.*

1. Introduction. The MF is the acronym for "Modified Fourier". This is a name of modern steganographic method developed at Lublin University of Technology, Institute of Computer Science. This method deals with hiding valuable information in other data that has no value or is insignificant and has very low value. A core of this method is based on the Fourier transform.

[1] Faculty of Electrical Engineering and Computer Science, Institute of Computer Science, Lublin University of Technology, Poland.

The MF method allows gaining a good robustness to compression, filtration and sound parameter change. The information is hidden by frequency spectrum strips values change. To avoid introducing audible interference the masking effect is used. MF method allows hiding one bit of additional information in one signal block (block is one signal fragment). It allows hiding several dozens bits in one second long recording. It is enough to realize secret communication, but bigger steganographic capacity will allow using smaller carriers to send messages and gives larger possibilities [5]. This article describes the MF method algorithm and the masking effect usage. On the base of the presented method the possibilities of steganographic capacity improving are described.

2. Masking. Masking is the phenomenon which causes human auditory system inability to record some sounds (masked) because they are "overwhelmed by other sounds (masking sounds)" [2,6].

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

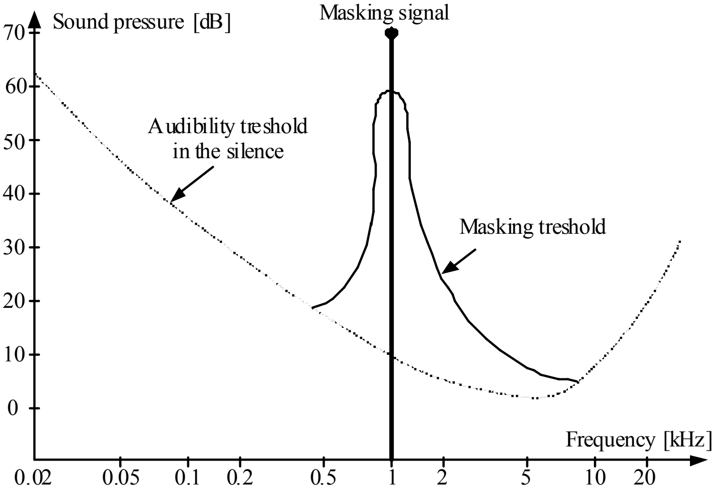

Figure 1. **Simultaneous masking threshold for 1 kHz sinusoidal masking signal while masking the "pure" sound [1]**

Using the same masking model would lead to creation of a 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 is necessary to develop an independent masking model. The research shows 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:

$$W_g \le (a-(f_{\max}-f)^2/b)*W_{\max}, \tag{1}$$

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 a masked strip.

Additionally it is important to choose strips placed next to a masker strip, so the range of strips possible to use by projected method is limited by values form the key (f_{dif1}, f_{dif2}). Changes introduced to a stegocontainer cause in spectrum changes, so it is worthy to leave some strips values unused to improve robustness. These values are placed between lines marked W_g and W_d on Figure 2. This figure shows how strips possible to use are chosen. On it the curve W_g is created after substituting the value of $a = 0.6$ and $b = 30000$ into equation 2. W_d is calculated by subtracting W_{max}*0.1 from the W_g value. Strips which can be used to hide data in are marked dotted.

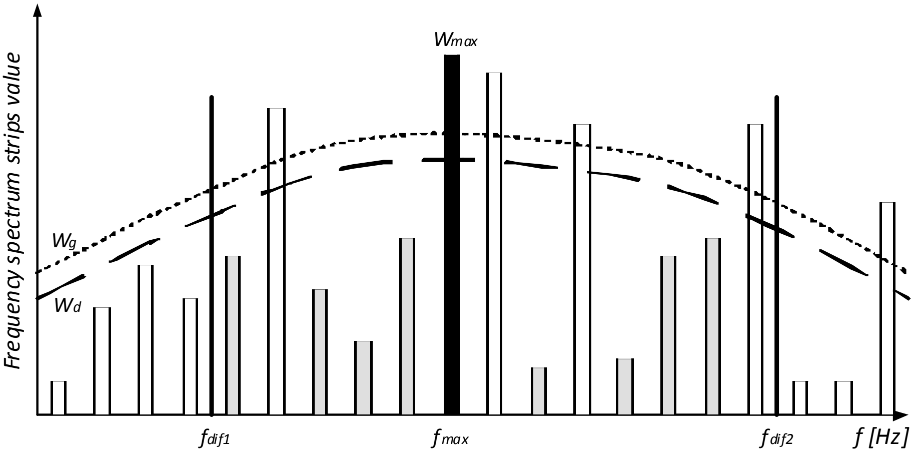

Figure 2. **Choosing strips to hide data in**

The dotted curve on Figure 2 sets the masking threshold, below which the changes made to a signal are inaudible. In the developed algorithm the W_d curve determines the maximum value of the modified sound frequencies and influences the choice of the used frequency bands used. If any strip value is placed in unused range its value has to be reduced to the W_d level. It is an additional advantage, because without knowledge of its course a person trying to read the attached message is not able to determine which bands of spectrum are used to hide additional information.

3. The MF method. Because of the fact that it is possible to hide only one bit of information in each signal fragment, it is necessary to divide the whole signal into smaller fragments (blocks). We do it in the time domain by taking the defined amount of signal samples. The following fragments are processed to hide one bit of a hidden sequence in each fragment. Processed sound fragment is transformed using DFT. The sound amplitude spectrum is computed from the result. This spectrum is analysed in order to find the strip with the highest value (a salient point, Kim, 2005). This strip is marked p_{max}, while its value is marked W_{max}. This strip corresponds to frequency fmax having the highest ratio in the signal, so it can be treated as a masker signal. Two spectrum strips are chosen from the masked range. Those strips are marked p_1 and p_2, their values w_1 and w_2 their frequencies f_1 and f_2 respectively, and will be used for hiding a bit of information. The choice of strips depends on a steganographic key. For the strip to carry information it must fulfil specific conditions:

- to be placed in the distance range (F_{dif1}, F_{dif2}) from f_{max},

- to have a value not greater than determined by the dependence (2):

$$W_n \le (a-(f_{\max}-\frac{f_n}{b})^2/b)*W_{\max}. \qquad (2)$$

Values F_{dif1}, F_{dif2}, a, b, come from the steganographic key, f_n is the frequency corresponding to the n-th strip.

Strips that fulfil the above conditions are placed in the table according to the sequence, determined by the key. Then, in sequence, they are checked to choose a pair which allows for hiding the determined binary value. The chosen pair is used for attaching the bit of information. In case when there are some neglected strips in front of the chosen one in the table, their values are modified in such a way that does not fulfil the dependence (2).

Next, the difference of values for strips p_1 and p_2 is calculated in order to determine whether it is as expected or any modification is needed. The expected value difference (R) is calculated on the basis of the steganographic key, which contains R_p value determining the ratio of R to the maximum value W_{max}. Value of R is calculated by the equation (3):

$$R = W_{\max} * R_p \qquad (3)$$

This solution allows adapting the power of modification to the signal strength and enables using all signal blocks. Hiding of the bit b in the signal means signal transformation in a way which fulfil dependence (4).

$$\begin{cases} |w_1 - w_2| \ge R, dla\ b = 1 \\ |w_1 - w_2| \le \beta, dla\ b = 0 \end{cases} \qquad (4)$$

where β is the value in the key determining the maximum range of the random value added to the calculated strip value.

Once the above dependence is met, the fragment is transformed back into the time domain with the use of the inverse Fourier transform (IDFT) and placed in the signal instead of the original fragment.

The following algorithm describes how the bit of information b=1 is being hidden in a signal:

- DFT is used to transform the signal, resulting in obtaining the vector of complex values Y_c,

- absolute value of vector $Y_r = |\ Y_c,|$ is computed,

- maximum value $W_{max} = max\,(Y_r)$ is determined in Y_r,

- difference $R = W_{max} * R_p$ is computed,

- positions of f_{max} of the max value strip p_{max} and the strips meeting the conditions for carrying hidden information are calculated,

- strips p_1 and p_2 are meant to carry the hidden data and are chosen, their values w_1 and w_2 are determined,

- on the basis of the key the maximum allowed value for each of the two chosen strips is calculated: w_1 allowed and w_2 allowed,

- *if* $|w_2 - w_1| \geq R$ then we finish the algorithm (values of both strips are correct),

- *if* $|w_2 - w_1| < R$ then we determine which of the strips has the greater value and which one has the smaller value and we mark them respectively w_w and w_m. After this, we calculate target values of the strips:

- *if* $w_m/\theta_{max} + R \leq w_w$, then $w_m = w_w - R - rnd(\beta)$, ($rnd(\beta)$ is the function that returns the random value from the range <-β, β>, θ_{max} is the maximum value allowed to be used to divide the strip value during its reduction),

- *if* $w_m/\theta_{max} + R > w_w$, then $w_m = w_m/\theta_{max}$, $w_w = w_m + R + rnd(\beta)$,

- next, the Y_c vector is updated on the basis of the calculated values (the phase is preserved as in the original signal),

- the updated vector Y_c is transformed into a signal in the time form by IDFT.

When it is necessary to change the values of the strips, the strip of the lesser value is modified first. Consequently, the amplification of the second strip is reduced. Thus, the power of the second amplified frequency is reduced, which results in distortion that can be masked in an easier way. Due to the fact that zero values almost do not appear in the signal spectrum, the author decided that the value of strip having smaller value reduction will be done by dividing it by a value from the range $(1, \theta_{max}>)$. Value θ_{max} is defined in the steganographic key. It allows avoiding introduction of zero value strip.

In order to obtain higher steganographic capacity of a signal, it should be divided into blocks. Successive bits of concealed information should be attached to those blocks. In the next step, the blocks should be combined [3, 4].

4. Increasing steganographic capacity. Bigger information capacity gives us more possibilities in the information protection domain [7, 8]. In the MF method only one bit can be hidden in each block. It is possible to boost the capacity. It can be done in 3 different ways:

- by bigger number local maxima usage;
- hiding more bits in one maximum neighbourhood by:
  - using one pair of strips;
  - using more than two strips;
- combined methods.

It is possible to use bigger number of maxima to determine the areas to hide additional bits of data. A sound signal spectrum can be any shape. It is obvious that there exists a lot of local maxima. Almost all of them can be used to point the area to hide additional data. As we know the MF method uses the strip having biggest value neighbourhood to hide one bit of data. There is no necessity of the strip having biggest value usage. It is enough if a chosen strip has bigger value than strips in its neighbourhood, and its value is big enough to find it with 100% certainty. It gives us opportunity to use bigger number of maxima. It is necessary to find the way of determining whose maxima will be used.

The first way is to use all maxima which have bigger values than the one given in steganographic key. The possible problems are:

- How to adjust the value in a steganographic key to be suitable for all the signal fragments? As we know all signal fragments have different spectrum. Strips existing in the spectrum have various values. In one fragment all values can be very big. In an other fragment values can be very small. Using constant value in a steganographic key do not allow determining maxima efficiently. It is better to use the ratio coefficient in a steganographic key. Next one of the parameters taken from the signal fragment (for example, the average value of strips existing in a processed sound fragment) can be multiplied by this ratio coefficient to calculate the final value used to determine local maxima to use.

- The second problem is lack of knowledge on how many maximas can be used in each fragment. This information we obtain after processing a chosen fragment. This results in unpredictable steganographic capacity. This problem can be the reason for reducing the robustness for compression and other operations that are commonly used to modify the sound signal. The reason are changes that can influence the spectrum strips values. Some maxima can increase their values, some can decrease. It can result in a change of maxima number which will be recognized as used in hiding process. It can result in serious errors in a data extracted from the stegocontainer.

The problems presented above seem to be serious enough to try to apply other solution. It is possible to use the defined number of maxima in each sound fragment. The number of used maxima will be a part of a steganographic key. In each fragment we have to find the determined number of maxima. To be able to find the same maxima in the decoding process and ensure good robustness we can use the next maxima having biggest value. Of course, we can not easily find some amount of strips having the biggest value. It is because each strip has to have big enough neighbourhood to hide data. It makes us respect the condition that between strips treated as local maxima has to be a distance at least as big as demanded by the method to hide additional data in the all strips neighbourhood. Hiding data in one local maximum neighbourhood can not influence the other local maximum neighbourhood.

Hiding more bits in one maximum neighbourhood is possible by:

- Hiding more bits with one pair of spectrum strips. It is possible to obtain by using intervals in differences between used strips values. The method principle is the same as in the MF method. But it is different in the strips values difference. If there is a difference between strips values in the MF method it is equal to hiding bit having value 1. In the presented modification we divide the difference into smaller ranges. For example, if we want to hide two bits, we have to ensure at least one range for each bits combination. With two bits we obtain 4 combination of their values: 00, 01, 10, 11. To each of them we assign the range of strips values difference. For example, the combination 00 will be represented by strips values difference ranging from 0 to 0.25*R, where R is the difference calculated according the MF method while hiding bit having value 1. The combination 01 is assigned to the range (0.25*R, 0,5*R). In the same way we can determine ranges for the rest of combinations. The problem can appear after introducing changes to the sound signal. Some spectrum strips values can be changed. It can result in moving strips values difference from one range to the other one. It will increase the bit error rate [9]. It is profitable to introduce intervals between defined ranges. For example, the first range can include values ranging from 0 to 0.15*R. Values ranging from 0.15*R to 0.30*R can be unused. It will boost the method robustness. Of course, applying this solution will negatively affect the robustness in comparison with the MF method. The robustness decrease will be proportional to the number of bits combination hidden with one strips pair usage.

- Bigger number of spectrum strips usage. It is possible to use two or more spectrum strips pairs to hide additional data. Each pair can be used to hide one bit of additional data. We use here the same algorithm as in the MF method. First we determine suitable pairs of strips. Next, each pair is processed independently to hide additional bit of data. It is done in the same way as in the original MF method. This modification will introduce more significant changes to the signal. It is necessary to be careful not to exceed the masking threshold.

The term "combined methods" means that we can combine solutions presented above to obtain the method having bigger steganographic capacity with modifications presented above usage. We can combine them in various ways that allow for desired steganographic capacity. Using these combinations we have to be careful to keep the appropriate level of transparency and hidden data robustness.

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

The size of the value changes of spectral strips depends on the value of the largest strip in the spectrum acting as a masker. This allows obtaining an optimal solution for both robustness and adaptation of ongoing changes in the amplitude of a signal in the selected part of this signal and to use all the fragments to hide additional information, regardless the volume. It is worthy to develop the MF method to boost its steganographic capacity to make it more useful and convenient to realize hidden communication.

References:

1. *Cvejic N.* Algorithms for audio watermarking and steganography, Oulu University Press 2004.

2. *Garay A.* Measuring and evaluating digital watermarks in audio files, Master Thesis, 2002, Georgetown University, Washington, D.C.

3. *Koziel G.* Fourier transform and masking in sound steganography, Актуальні Проблеми Економіки, 12'2009, 2009.

4. *Koziel G.* Method of concealing information in sound based on Fourier transform and masking, Polish Journal of Environmental Studies, pp. 181-186, 2009.

5. *Laskowski M.* Critical Date Bugs and Their Impact On Computer-Based Economy, Актуальні Проблеми Економіки, no. 120, pp. 335-339.

6. *Mahbour R., Syed M.* Multimedia Technologies: concepts, methodologies, tools, and applications, London 2008.

7. *Milosz E., Milosz M.* Digital identity management in Polish SMEs, Actual Problems of Economics, No. 6, 2011, pp. 340-345.

8. *Juszczyk M.* Impact of human factor in data security. Actual Problems of Economics., No. 6, 2011, pp. 359-364.

9. http://pl.wikipedia.org/wiki/Bit_Error_Rate.

Стаття надійшла до редакції 16.01.2012.