8K

UDC 681.03

Koziel Grzegorz
Lublin University of Technology, Poland

Steganographic Methods in Information Protection

New information protection methods are necessary. Steganography seems to be great opportunity to replace or supplement the cryptographic methods. Steganography gives additional possibilities. It allows to keep in secret the communication fact and communicating sites personality. A lot of existing methods and the proposal of a new one are presented in the article.

Introduction

Steganographical methods are used in three main areas:
– hidden communication;
– watermarking;
– protections against optical discs copying.

Each use has different demands. In watermarking the robustness and high transparency of the attached data are demanded. Steganographic capacity does not have to be great but it is necessary to ensure enough space to save all used signatures. In hidden communication the most important is good transparency and good hide of data. It means that used method cannot introduce perceptible changes in the used carrier signal. Of course, big capacity of the method is very important. Features and statistical measures cannot be changed too. Of course, the best solution would be the method that offers all features: good transparency, robustness and capacity. Unfortunately we find that it is impossible. The best the situation is described by the triangle of conflict presented in Fig. 1.

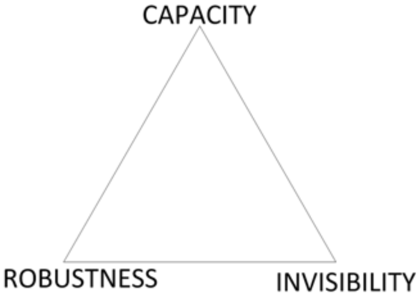

Figure 1 – Triangle of conflict

Steganographic method creator is limited by triangles edges. The methods properties must be placed inside the triangle. We can show them as a point inside the triangle. When we want to improve one of the properties we can do this only at the expense of other properties. For example if we want to gain more capacity, we have to lost some robustness and invisibility. This theory can be proved very easy on the example. If we want to obtain the maximum capacity, we have to use all data contained in the carrier. It means that we modify all bits of the container. Of course we lose all data previously existing in the container and completely lose the robustness. It is enough to change one randomly chosen bit to destroy the hidden data. To obtain more invisibility we have to reduce the amount of changed bits. It means that we lose some capacity. If we want to gain more robustness we have to allocate some additional bits in this. Thus we reduce the amount of bits available to hide data, we reduce the capacity or we have to use some bits, which haven't been changed yet. It causes the bigger changes introducing what results in poorer transparency.

Each application demands its own set of features, so it is necessary to ensure the possibility of obtaining the various feature sets. It is possible by using different methods.

Steganographic methods due to the mode of action can be divided into six groups [1].

1. Substitution method, involving the replacement of redundant data carrier by concealed information.

2. Transformation metho, involving the signal container transformation to the frequency domain and include information by modifying the transform coefficients.

3. Method of spread spectrum, using the entire frequency spectrum to the dispersion of hidden data, which are also scattered throughout the media.

4. Statistical methods, hiding data by modifying the statistical features of the media.

5. Distortion methods, running through the introduction of signal distortion to the container; to read the attached information is necessary to compare the stegocontainer with the original.

6. Method of container generation, creating stegocaontainer on the concealed information base. The goal is to obtain the container best suiting to the hidden data.

Each group of these methods allows to obtain a different set of features. Usually each group allows for one feature easy improvement and does not allow to improve other features so easily.

Substitution methods

Substitution methods are most often realized by amplitude modification method, which is known as least significant bit (LSB) method. It is well known and popular in communication as well as in watermarking [1]. Least significant bits of audio samples, which are not carrying valuable information but only quantization noise, are used for information concealment. Modifying value of those bits does 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 [1-3], 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 [4]. Shaping the characteristics of additional sequence in order to matching it with container signal is another possibility presented in [5]. 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 robustness of the method, but it is preformed at the cost of steganographic capacity.

In [2] 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.

Transformation methods

Transformation 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 [4]. Transform methods show high robustness to signal compression. Unfortunately, they are not robust for time scale modifications. The authors [6] present the method robust for desynchronization 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.

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 [4]. 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 is based on multiplying the signal of attached information with other, quasi-random signal with higher bit flow [2], [7]. 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, that results in spectrum compression and makes possible reading of the additional information. To read the information a key (used quasi-random sequence is indispensable), to keep distortions at low level, watermark signal power should not exceed 0,5% of container signal power.

Spread spectrum method is one of the better steganographic methods thanks not only to high robustness to detection, damage and deletion, but also to high steganographic capacity [4], [8]. 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 that improves robustness to detection and damage of hidden information.

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.

Statistical methods

Statistical methods are based on various statistic changes. The example of this type of method can be histogram technique presented in [7], [9], where authors 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 is not negative, A is 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 is 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 (1).

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

The authors [9], [10] 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 (2) in order to conceal a single bit of data.

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

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, the authors [9], [10] present the results for T=1.4, $\lambda=2.4$ i $P=40$, moreover they assume the possibility of correct watermark identification with 15% reading error rate. Using those values of coefficients allows 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%, lossy compression and jitter effect.

Distortion methods

Distortions methods introduce changes in randomly chosen parts of container. To read hidden data, it is necessary to compare the stegocontainer with the original carrier. The disadvantage of this method is the necessity of safe communication channel use to send the original files. The special example of this type method is interference removal methods, which hide information during the container repairing. It allows to hide data and improve the carrier quality in the same time. This type method was described in [11]. This method removes the impulse interference from audio recording. The interference is detected by neural network. Another networks are applied to repair: two different neural nets have been trained to remove interference. The approximate values of samples repaired have been determined by each of the different nets. During the process of adding to the recording values of the samples repaired the additional information coding algorithm was used. Data added has been converted to a binary form. We have assumed that adding value generated by the first net will correspond to the binary value one and adding value given by the second net will equal value zero. In this way it is possible to attach to the repaired recording additional information. The parameters of the resulting signal do not differ in quality from the signal which was the subject of only the repair, due to the fact that every process of repair allows to achieve only the approximate signal value. Using values generated by different nets does not introduce additional deformations as compared with values returned by one. In order to estimate errors interference was generated for the non-defective signal. This allowed to compare parameters of the tested signals [12], [13]. Mean square error and the signal noise ratio for the signal repaired by net #1 were respectively 0.027 and 21,6dB. For the signal repaired by net #2 the values were 0.026 and 21dB; and for the signal with added information 0.026 and 21,7dB.

Container generation methods

Conatainer generation methods work by creating the stegocontainer on the base of hidden data. It allows to obtain the stegocontainer having the best features set for defined data hide. Unfortunately it is very difficult to obtain the signal that makes a sense. Usually it is possible to generate abstract content which very often looks artificially. This is the reason that these methods do not gain the popularity.

MF method

MF is Fourier based method. It was designed to fulfill the necessity of creating robust methods to communicate. We use not only the ideal channels. Sometimes it is necessary to send stegocontainer through the communication channel where information is processed by compressing it or format changing. Very often the additional noise is generated. A lot of methods are not able to hide information in such a way to allow to survive the hidden information. Some of them have suitable robustness but steganographic capacity is not enough. In this case it is necessary to provide good robustness and steganographic capacity not less than several dozens of bits per second. The MF method presented in [14] meets these requirements.

Fourier transform-based methods, which hide information by changing frequency are successfully used in cases, where image is the data carrier. Due to high sensitivity of human ear to frequency changes, development of this method in sound was cancelled, as it was very hard to hide the presence of changes. Masked frequencies can be used for steganographic purposes to avoid this difficulties.

In MF method chosen sound fragment is transformed using DFT. Sound frequency spectrum is computed from the results. This spectrum is analyzed in order to find stripe with the highest value. This stripe is marked f_{max}, while its value is marked W_{max}. This stripe corresponds with frequency with the highest ratio in signal, so it can be treated as a masker signal. Two spectrum stripes are chosen from the masked range. Those stripes are marked f_l and $f_{2,}$ their values w_l and w_2 respectively and will be used to hide a bit of information.

Distance between both stripes and masker is defined by steganographic key. The difference of values between stripes f_l i f_2 is computed in order to define whether it has to be modified or is compatible with expectations. The expected value difference (R) is defined in the steganographic key. It can be given as constant (R_{const}) or as a percentage (R_p) of maximum value $W_{max.}$

Research showed the supremacy of the flatter solution due to adjustment the power of modification to the power of signal and the possibility of using all signal fragments. Bit *b* is hidden in the signal by transforming the signal to fulfill the following dependence (3):

$$\begin{cases} w_1 > w_2 + R, dla\ b = 1 \\ w_1 + R < w_2, dla\ b = 0 \end{cases} \tag{3}$$

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

1. DFT is used to transform the signal, resulting in obtaining vector of complex values $Y_{c.}$
2. Absolute value of vector $Y_r=|Y_c|$ is computed.
3. Maximum value $W_{max}=max(Y_r)$ is determined in Y_r.
4. The position of maximum value, f_l and f_2 is determined.
5. Difference $R= W_{max}* R_p$ is computed.
6. If $w_l<w_{2,}$ then values of f_l and f_2 stripes are swapped.
7. If $w_l<w_2+R$, then:
   a. if $w_l>0.3*w_2+R$ then factor $x=(w_l-R)/w_2$ is computed. Value of f_2 stripe is then divided by that factor;
   b. if $w_l<0.3*w_2+R$, then value of f_2 stripe is divided by 2, new factor $y=(w_2+R)/w_l$ is computed for new value w_2, then value of f_l stripe is multiplied by y.
8. The updated vector Y_c is transformed into signal in the time form by IDFT.

When it is necessary to change the value of the stripes, the stripe of the lesser value is modified first. This results in reduced amplification of the second stripe. Thus power of the second amplified frequency is reduced, which results in distortion, which can be masked in an easier way.

The value of the smaller stripe can be reduced to zero. Due to the lack of zero values in the signal spectrum, the author decided that it would be adverse because of the possibility of spotting them during signal frequency analysis.

In order to obtain higher steganographic capacity of the signal, it should be divided into blocks. Successive bites of concealed information should be attached to those blocks. In the next step, the blocks should be combined together.

There are often discontinuities at the block connections, which introduce interferences in the form of cracks. Leveling of the discontinuities is necessary to eliminate them. The author proposes usage of connection blocks put between information-carrying blocks.

In the following algorithm, information-carrying blocks are marked as fr1, fr2, connecting block as s, number of samples in s block as k.

Blocks are placed as following: fr1, s, fr2.

The algorithm of the connection:

1. Information is concealed in blocks fr1 and fr2.
2. The difference r1 between the last sample of block fr1 and corresponding sample of original signal is computed.
3. The difference r2 between the first sample of block fr2 and corresponding sample of original signal is computed.
4. S block is copied to s1 block, r1 is subtracted from each samples of s1.
5. Value of each sample is multiplied by w=k/sample index, indexes are the subsequent numbers starting from 0.
6. S block is copied to s2 block, r2 is subtracted from each samples of s2.
7. Value of each sample is multiplied by its index.
8. Values of samples of connection block s' are computed according to formula (4):

$$s3(i) = \frac{s1(i) + s2(i)}{k} \quad , \; i = 0,1,2,...k \tag{4}$$

where i is sample number.

9. The following blocks are put into the result signal.

The use of connecting blocks allows acquiring solid result signal. The cracks are completely removed.

In this method original carrier is not needed to read the concealed data. Only the knowledge of the steganographic key is essential. This key contains such data as: placement and size of information-carrying blocks, distances of modified stripes from the stripe with the highest value and applied value difference (R_p).

In order to read the hidden information, the position of the stegocontainers has to be determined. Each stegoconteiner should be transformed using DFT. The position of modified stripes in the result spectrum should be determined. The difference R' of their values should be tested. The value of the maximal stripe W_{max} should be determined as well. In the next step, value of the hidden bit *b* can be read according to dependence (5):

$$\begin{cases} b = 1, \; gdy \; R' \geq 0.6 * R_p * W_{\max} \\ b = 0, \; gdy \; -R' \geq 0.6 * R_p * W_{\max} \\ b = -1, \; gdy \; |R'| \leq 0.6 R_p * W_{\max} \end{cases} \tag{5}$$

b=-1 means, that value reading is uncertain.

As multichannel recording is currently used most frequently, the additional channels can be used to introduce error correction codes. Considering two-channel signal, the copy of the information can be put in the second channel in order to make the correct reading of the hidden data possible in case of damaging one of the copies. Multichannel recording gives more opportunities, as one error correction codes can be put in one channel, while the remaining channels can be used to carrying information.

Presented method allows to obtain steganographic capacity up to 84 bits per second for stereo signal. This method allows to obtain good resistance. The bit error rates [15] measured after changing format to other are presented in Table 1.

Table 1. The MF method robustness to sound processing.

Operation or used sound format	BER [%]
Ogg	3,60%
mp3	14,00%
Aac	10,00%
Ape	0,00%
wma quality=98%	0,90%
wma quality=75%	5,00%
wma quality=50%	8,60%
wma quality=25%	12,70%
wma quality=10%	15,40%
Sampling frequency reduction to 22kHz	0,00%
Sampling frequency reduction o 11kHz	0,00%
Sampling frequency reduction 8kHz	0,50%
Bandpass filtering 1Hz-15kHz	1,40%
Bandpass filtering 1Hz – 5kHz	3,20%
Bandpass filtering 1Hz – 2kHz	8,10%
Bandpass filtering 40Hz – 20kHz	23,10%
Bandpass filtering 80Hz – 2 kHz	36,20%

Increasing capacity of the MF method

There is possibility of increasing the MF method steganographic capacity. It can be done by hiding more than only one bit inside two spectrum strips. But it will cause the same situation as introduced changes value decrease. The method will not be as robust as previously. It will happen because after the sound processing operations apply the stripes values change. If the value corresponding with the one bit of hidden data is greater then it can survive bigger spectrum change.

The second possibility of increasing capacity of methods is to use more stripes inside the area masked by the biggest stripe. Of course, it is necessary to develop a special algorithm to choose stripes to use because each time different number of stripes is masked. Algorithm implemented in the MF method will not work. Different solution is necessary.

The third possibility is to use local maximas as maskers. Then it is possible to use the same algorithm and solutions developed in the MF method to hide more data. It is necessary to determine how many local maximas we can use and which conditions it have meet. The proposition of the algorithm of hiding data in plenty maximas looks as follows:

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

1. DFT is used to transform the signal, resulting in obtaining vector of complex values $Y_{c.}$
2. Absolute value of vector $Y_r=|Y_c|$ is computed.
3. Maximum value $W_{max}=max(Y_r)$ is determined in Y_r.
4. The position of maximum value, f_1 and f_2 is determined.
5. Difference $R= W_{max}* R_p$ is computed.
6. If $w_1<w_{2,}$ then values of f_1 and f_2 stripes are swapped.
7. If $w_1<w_2+R$, then:

a. if $w_1>0.3*w_2+R$ then factor $x=(w_1-R)/w_2$ is computed. Value of f_2 stripe is then divided by that factor;

b. if $w_1<0.3*w_2+R$, then value of f_2 stripe is divided by 2, new factor $y=(w_2+R)/w_1$ is computed for new value w_2, then value of f_1 stripe is multiplied by y.

8. The maximum distance (d_{max}) between stripe having value 1 and the least masked stripe is calculated.
9. The area ranging to $2*d_{max}$ from the used masker is marked as “unusable”.
10. In the area that is not marked as “unusable” the biggest stripe is determined.
11. The determined value is a new masker.
12. The bit of additional data is hidden in the masker neighbourhood according to the steps 3-7.
13. Repeat steps 9-12 the specified number of times.
14. The updated vector Y_c is transformed into signal in the time form by IDFT.

Summary

The different steganographic methods analysis showed that people failed in trying to create the ideal steganographic method, although plenty of various algorithms exist. Each of the presented solutions has its advantages and defects. This is due to the contradictory requirements between steganographic capacity, transparency and robustness. Improving one of the listed parameters we cause deterioration of the others. This rule concerns each steganographic method.

It is impossible to rate which method is the best because each method has its own individual set of properties and features. It is necessary to choose a method for the individual application. The chosen method has to address the needs of application.

The MF method fills the blank between the watermarking methods and communication methods whose are not robust. The proposed improvement allows to obtain greater steganographic capacity of the presented method.

References

1. Garbarczuk W. Podstawy ochrony informacji / W. Garbarczuk, A. Świć. – Politechnika Lubelska, 2005.
2. Dugelay J.L. A survey of current watermarking techniques / J.L. Dugelay, S. Roche // Information hiding: Techniques for steganography and digital watermarking. – Boston, 2000. – P. 212-148.
3. Johnson N.F. A survey of steganographic techniques / N.F. Johnson, S.C. Katzenbeisser // Information hiding: Techniques for steganography and digital watermarking. – Boston, 2000. – P. 43-48.

4. Katzenbeisser S. Information Hiding Techniques for Steganography and Digital Watermarking / S. Katzenbeisser, F.A.P. Petitcolas. – London, 2000.
5. Czerwinski S. Digital music distributionand audio watermarking / S. Czerwinski, R. Fromm. – Berkeley, 1999.
6. Wang X. Novel Synchronization Invariant Audio Watermarking Scheme Based on DWT and DCT / X. Wang, H.A. Zhao // IEEE Transactions on signal processing. – 2006. – Vol. 54.
7. Kirovski D. Robust cover communication over a public audio channel using spread spectrum / D. Kirovski, H. Malvar. – Pittsburgh, 2001.
8. Tomaszewski M. Analiza algorytmów steganograficznych / Tomaszewski M.
9. Xiang S. Time-Scale Invariant Audio Watermarking Based on the Statistical Features in Time Domain / S. Xiang, J. Huang, R. Yang // Artificial Intelligence and Lecture Notes in Bioinformatics. – 2007. – P. 93-108.
10. Xiang S. Audio watermarking robust against time-scale modification and MP3 compression / S. Xiang, H. Kim, J. Huang. – http://ieeexplore.ieee.org
11. Kozieł G. Zastosowanie Sieci Neuronowych w Steganografii Dźwięku / G. Kozieł // Informatyka stosowana, planowanie, 2007.
12. Rutkowski L. Metody i techniki sztucznej inteligencji / Rutkowski L. – PWN, 2005.
13. Tadeusiewicz R. Elementarne wprowadzenie do techniki sieci neuronowych z przykładowymi programami / Tadeusiewicz R. – Akademicka Oficyna Wydawnicza PLJ, 1998.
14. Kozieł G. Properties of a New Fourier Transform-based Steganographic Method / G. Kozieł, V. Harbarchuk // Artificial Intelligence. – 2010.
15. http://pl.wikipedia.org/wiki/Bit_Error_Rate
16. Bassia P. Robust audio watermarking in the time domain / P. Bassia, I. Pitas. – Rhodes, 1998.
17. Techniques for data hiding / W Bender, D. Gruhl, N. Morimoto, N. Lu // IBM system Journal. – 1996. – № 5.
18. Bogumił D. Cyfrowe znaki wodne odporne na kompresję JPEG / Bogumił D. – Warszawa, 2001.

Г. Козиел

Стенографические методы защиты информации

Новые методы защиты информации являются необходимыми. Стенография может заменить или дополнить криптографические методы. Она предоставляет новые дополнительные возможности и позволяет сохранить в секрете факты коммуникации, а также некоторые аспекты личной коммуникации. В статье описывается много методов и предложен новый метод защиты информации.

Г. Козіел

Стенографічні методи захисту інформації

Нові методи захисту інформації є необхідними. Стенографія може замінити або доповнити криптографічні методи. Вона надає нові додаткові можливості і дозволяє зберегти в секреті факти комунікації, а також деякі аспекти особистої комунікації. У статті описується багато методів і запропонований новий метод захисту інформації.

Статья поступила в редакцию 31.05.2011.