Scientific Journal of Riga Technical University
Computer Science. Applied Computer Systems
2011
Volume 47

Unified Evaluation System for Audio Steganography Methods

Andrew Yershov[1], Roman Karpelcev[2], [1-2]*Riga Technical University*

***Abstract* – The interest in the digital steganography grows together with the rise of amounts of multimedia data exchanged over the Internet. This growth provides steganography with new possibilities and opportunities for data hiding. The information hiding in audio streams is considered especially promising due to audio data popularity and possibilities to hide data within audio signals. There are many data hiding methods. The steganography is used to process audio streams, and the new methods are constantly emerging. These methods have different applications and targets, features and properties. This paper presents the Unified Evaluation System (UES) for evaluation, comparison and classification of audio steganography methods proposed by the authors. UES is a set of calculation principles, which are especially combined for audio steganographic methods. The system's outcomes provide conclusions in order to determine advantages/disadvantages of the methods and to define the audio steganography methods as the most suitable for each particular case.**

***Keywords* – audio steganography, audio stream, compression, attack.**

I. Introduction

In audio steganography the secret messages are being embedded in digital sound by slightly altering the binary sequence of a sound (audio) file. Embedding secret messages in digital sound is usually a more difficult process than embedding messages in other media, such as digital images. In order to conceal secret messages successfully, a variety of methods for embedding information in digital audio have been introduced, e.g. LSB coding, parity coding, spread spectrum, echo hiding, phase coding. These methods range from rather simple algorithms that insert information in the form of signal noise to more powerful methods that exploit sophisticated signal processing techniques to hide information. So a variety of audio steganography methods provides users with a wide choice and makes the technology more accessible to everyone. But on the other hand, it raises a problem of method's selection that best fits the required specifications. This paper presents the individually developed system that is intended to solve the above mentioned problem. The system is based on 6 different criteria that allow evaluating steganographic methods that are used for processing audio streams. Evaluation scales are provided for objective evaluation and comparing of the criteria.

II. The Evaluation Criteria

In the following chapter the criteria on which the evaluation system is based are introduced. Each criterion has explanations about its essence along with the reasons for its use.

A. Capacity

Capacity is a value that defines how many bites of a secret message can be embedded in the data stream container per one second. In the evaluation system the acceptable capacity of the method is measured by bits per second. The higher the number of bits per second that can be embedded in the audio stream the higher the capacity is [1]. The higher value takes the advantage in this criterion. In the further text the value of criterion is labelled with a variable *C*.

We, the authors of this paper, emphasize that different capacity values can be achieved for the same method by using different implementations, embedding settings, and data containers. In this case other parameters like the values describing robustness and relations between signal and noise would be resulting from the implementation or taken from the settings of the same method that were achieved by using data container with the same qualities. One has to be especially careful with the discretization frequency of the container and has to make sure that is the value is same by checking and comparing. It is important because the capacity of several methods is linearly dependent on the audio stream's discretization frequency (for example, implementation of Least Significant Bits), but at the same time others are less dependent. Different methods' dependency from the discretization frequency of stream is the reason why the running capacity criteria is not expressed as bits per second on one Hertz (b/s/Hz), but as bits per second.

B. Robustness versus data transmission types

There are several types of an audio stream transmission. The goal of this criterion is to show how the steganographic method can endure the transmission offered below and different kinds of transformations and conclude the evaluation dependently on that. The values of the criteria can be labeled with variable *T*.

Each method fits one of the following descriptions:

1. The transmission must happen in digital environment without recoding.
2. Decoding in different audio formats is possible; transmission is performed in digital environment.
3. Transmission through ideal noiseless analog channel is possible with later recoding in digital format.

4. Transmission with stream recording by using microphone.

When evaluating the method one must choose a description that most fully represents characteristics of the method. According to the first description, for example, there is copying of the coded file from one computer to another, or there can be a digital streaming without decoding – the stream is not changed. The decoding belongs to the second description of another format that changes some of the sound characteristic quantities but absolute amplitude, sound phases and often also discretization frequency remain unchanged. The third description means that embedded data with the method remains preserved also without the transmission which changes the absolute amplitude and characteristic quantities of the previous discretization. After such transmission the sound is discretized and digitalized over again. The fourth description means that all the information connected with discretization, amplitude and phase as well is lost and other signal distortions are possible along with outer noises. A typical example is transmission of the signal through the radio broadcast when the signal is recorded by microphone.

The evaluation of the method according to the most suitable description is described in the Table I. In the table the transmission types are arranged from the simplest to more complicate according to robustness. Each next type of transmission contains the possibility to use all other types. The descriptions are not linearly arranged in order to better describe the advantage of methods in further comparisons, especially in the relative comparisons described below.

TABLE I
VALUES OF *T* CRITERION

Nr.	Short description	Evaluation
1	Without stream changes	1
2	Decoding in digital environment	3
3	Transmission through the ideal noiseless analog channel	6
4	Radio broadcast	8

One have to note that the evaluation of this criterion does not show the persistence of the method against attacks whose goal is to destroy the hidden message. The criterion of robustness against data transmission environment is provided to show possibilities and environments where the method can be used.

C. Robustness versus attacks

The robustness of methods is exposed not only in streams transmissions or decoding the stream in different environments, but also in attacks. Attack is considered to be a deliberate attends to destroy a hidden message. Expression "destroying" has two meanings in context of steganography: 1) to delete the hidden message from the stream, 2) to change it in one or another way which does not allow the recipient to receive this message [1].

One of known attack kinds is adding noise to the audio stream [2]. By adding noises with concrete characteristic values is possible to bother significantly the extraction of the hidden message. The added noise may not influence signal reception in human hearing system but can rewrite the bits of the hidden message or increase the number of wrongly embedded bits.

It is offered to label the variable that describes the robustness against the attacks as A. This value represents the publicly known number of attacks which can destroy messages embedded with appropriate steganographic methods. The smaller is the value, the better method is considered to be protected against attacks. We point out that during the research only four different attack kinds were detected. So the worst possible value is 20. It is freely chosen value (for simplification of calculations), because the number "20" is 5 times larger than the number of attacks to data hidden in audio streams. This limit is necessary in those cases when it isn't possible to get the data about different kind of attack.

This characteristic quantity was described as a separate criterion because we think that there is a notable difference between distortions of transmission environment and deliberate attacks. The high evaluation of method in this criterion most probably means higher evaluation in the previous but not necessary the other way round. In cases when ability to endure analog transmissions is essential and at the same time necessity to have protection against the attacks is not vital, evaluation of divided criteria will let more objectively to determine the most suitable methods.

D. The added noises

The application of any audio steganographic methods changes the original signal and adds noises in it by embedded message in the data container stream. The amount of added noises influences the fact how the human hearing system receives the changed signal and whether it can separate original stream from the changed one.

In the signal theory the characteristic quantities are placed that allow evaluating the amount of noises in a signal [3]. These quantities are often connected with the signal and noise ratio that is marked as SNR (*Signal-to-Noise Ratio*). The signal and noise ratio can be applied to any stream signal, including audio, and shows how many times stronger the desired signal of the stream is than the noises in the stream. If the value of this ratio is larger than 1, it means that desired signal power is greater than the power of noise. This ratio would be infinite for the perfect signal without noises [3].

We think that the simple SNR is the most advanced value quantity to determine an approximate quantity of added noises along all length of the stream and choose not to take into account the values of the noise ratio, for example, like *PSNR* (*Peak Signal-to-Noise ratio*). SNR ratio can be calculated as ratio of signal powers or as the square of signal amplitude divided with the square of noise amplitude [3]. By using the characteristics of logarithms the value of SNR in decibels is expressed with (1), where A_s is the desirable signal amplitude and A_n is the noise amplitude:

$$\mathrm{SNR}_{\mathrm{dB}} = 20\log_{10}\frac{A_S}{A_n} \quad (1)$$

Because the ratio value of signal and noise can significantly vary for different algorithms and methods, it is expressed in decibels (dB) in the logarithmic scale. In cases when SNR value will be found as linear digital ratio (further marked as *SNR'*) by using (2), one can compute the SNR value in decibels:

$$\mathrm{SNR}_{\mathrm{dB}} = 10\log_{10} SNR' \quad (2)$$

We offer to leave the SNR label for the variable that will describe the evaluation in this criterion. The bigger is the SNR value, the better is the evaluation.

E. Intensity of extraction errors

Embedding the message in the stream and protection in the signal transmission time is only a part of the total data hiding process. Every message, which was embedded in the audio stream, has to be extracted after receiving via the transmission channel. Depending on the method used, stream transmission environment and other circumstances, the part of embedded message could be lost or wrongly extracted/decoded [4]. We assume that due to the concept of hidden message successful transmission the intensity of extraction errors is an important variable. So this value is offered as one of the criteria for the evaluation system. The intensity of extraction errors depicts how many embedded bits are wrongly extracted after receiving the stream. The intensity is relative against the total amount of transmitted data.

The variable *I* is used to label the value of this criterion. We offer formula (3) for its calculation, where ε is a number of mistakenly defined bits in the message and *N* is a total number of bits in message.

$$\mathrm{I} = \frac{\varepsilon}{N} \quad (3)$$

The value of *I* is described with value from 0 till 1. In practice 1:1 ratio will not usually be achieved because it would mean that none of the hidden message bits is extractable. And therefore the data hiding method would not hide any data. Also it must be pointed out that the value of the ratio, that equals 0, is hardly reachable in practice. So we turn our attention to the fact, that if the error intensity is larger than 0, it is possible to fully extract the hidden message. By using and adding to message *ECC* (*Error correcting code*) during embedding process [4], the errors of bits are possible to correct till a definite level. The usage possibilities of error correction codes must be held in the mind when evaluating and comparing methods according to the criteria of error intensity.

The lower evaluation gained in criterion a better it is presumed to be. Like in the criterion of added noises, if evaluating methods, the constant testing and exploration of methods is not foreseen, the value of this variable can be gained from existing research [1], [2].

$$\mathrm{I} = 1 - R \quad (4)$$

$$\mathrm{I} = 1 - \frac{R}{100\%} \quad (5)$$

In the scientific researches there is mentioned a related value, that is called the *recovery rate*. The recovery rate represents how many bits from the number of embedded bits in the audio stream were possible to extract and identify successfully. The intensity of extraction errors *I* can be calculated by using (4) or (5), if the recovery intensity R is expressed in percent.

F. The support of audio formats

The audio stream can be encoded and transmitted in different formats and the possibility of usage of different audio stream coding formats can be taken to be as a criterion in method comparison. Because the evaluation system offered in this paper is meant for method compartment and does not foresee evaluation of concrete software, so the evaluation of criteria does not require survey of the appropriate audio format standards, but their classes.

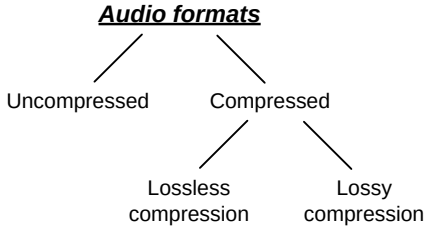

Fig. 1. The division of audio stream coding formats

The audio formats are divided (see Figure 1) in compressed and uncompressed classes. Compressed formats present as formats with lossless or lossy compression. One of the popular uncompressed formats is WAV LPCM format that is used for recording audio compact discs [5]. In the uncompressed formats each channel is stored separately and every reading is kept. In the compressed formats, on the other hands, the data are categorized, encoded or otherwise compressed in a way so that they take less memory volume than uncompressed sound. The audio channels in these formats can be divided or added to others; storing structure of reading can differ from uncompressed. Lossless compression algorithms (for example, FLAC [6]) differ with the fact that it fully keeps the original audio signal without changing its dimension and adding noises. Lossy compression algorithms (like MPEG [7]) transform the audio signal by leaving within possibility only sounds, which a human can hear, or the sounds that are essential in the original audio signal. If lossy compression algorithms are used with high degree of compression, it can also create hearable noises.

That is why there are three possible format choices (see Table II):

TABLE II
SUPPORT OF AUDIO FORMAT

Nr.	Short description	Points
1	Uncompressed audio	1
2	Lossless compression	1
3	Lossy compression	2

We offer to label the variable with an *F*. For every supported format the point number shown at the Table II is added to evaluation. If several formats are supported, the points will be summed up in evaluation. In this case the smallest possible value is 1 – only one of the formats is supported and the highest is 4 – all formats are supported. The evaluation scale gives larger value to lossy compression support, because lossy compression algorithms are much more popular between the users than lossless or uncompressed audio [8-10] and create greater difficulty in embedding hidden information in them – so we give it a better evaluation that the support of other format.

III. SYSTEM APPLICATION

A. Methods' comparison

According to the system specificity, one must choose methods that need comparison and prepare information about them and their characteristic quantities. In a case of incomplete information or if the user has a possibility to explore and analyze the methods himself, the equations are provided for different criteria to evaluate methods numerically.

If a value necessary for a criteria cannot be found in existing research and the user has no possibility to explore himself, one must presume that the lowest possible value will be given to that steganographic method and keep in mind that comparison according to this criteria cannot be objective.

We offer a tabular data representing method to compare absolute values of the criteria (see Table III):

TABLE III
PATTERN OF COMPARISON TABLE

Method\ Criteria	Name of method	Name of method
Capacity *C* (b/s)	…	…
Transmission types *T*	…	…
Attacks *A*	…	…
SNR (dB)	…	…
Error intensity *I*	…	…
Format support *F*	…	…

B. Unified relative evaluation and comparison

During the process of methods' comparison the user may have a wish not only to compare the methods using the provided table, but also relatively make common graphical representation for all methods.

The relative values of criteria are expressible in percents according to equations described below. Differently from the absolute values the greatest percentage always means better result. We think that if a method has not had a possibility to find or gain evaluation of some criteria, in the relative assessment the method must have 0% assessment and the absolute result gained in method criteria (before it was presumed that it must be the worst possible result) is not considered when calculating the relative values.

We point out that one of the evaluations of the criteria, the capacity criterion, is not only expressed in relative percentage but also changed and in the relative evaluation depicts logarithmically increasing value. The decision of using the logarithmic scale in the relative assessment is made because different methods may have very different capacities and their ratio would be expressed in hundreds and thousands. With a linear scale it would lead to small percentages for methods with low capacity and would not allow to compare them between themselves at the moment when a method with times greater capacity is compared to them. A logarithm with basis 10 was assumed by changing the values in the logarithmic scale – see (6).

Another important remark is connected with the fact that the error intensity in this comparison is also relative according to other methods that is why 100% result can be achieved with a error intensity bigger than 0.

Relative evaluation for each criterion is labeled with the same variable as the absolute evaluations, by adding the lower index r to variables that show the relativity of the assessment. The evaluation variable with index min or max means accordingly the smallest or the biggest absolute evaluation between all methods that are analyzed. The smallest and biggest values are presumed to be mathematically compared evaluations.

1. Relative capacity:

$$\mathrm{C_r} = \frac{\lg C}{\lg C_{\max}} \times 100\% \tag{6}$$

2. Relative robustness of transmission environment:

$$\mathrm{T_r} = \frac{T}{T_{\max}} \times 100\% \tag{7}$$

3. Relative robustness versus attacks:

$$\mathrm{A_r} = \begin{cases} 100\% - \dfrac{A - A_{\min}}{A_{\max} - A_{\min}} \times 100\% \\ \mathrm{A_r} = 100\%, \; ja \; A_{\max} = A_{\min} \end{cases} \tag{8}$$

4. Relative signal and noise ratio:

$$\mathrm{SNR_r} = \frac{SNR}{SNR_{\max}} \times 100\% \tag{9}$$

5. Relative recovery intensity:

$$\mathrm{I_r} = \frac{1-I}{1-I_{\min}} \times 100\% \quad (10)$$

6. Relative format support evaluation:

$$\mathrm{F_r} = \frac{F}{F_{\max}} \times 100\% \quad (11)$$

We point out that relative assessment is meant for better comparison of the methods and do not recommend deciding and choosing methods only according to results of a relative assessment. For more accomplished evaluation and comparison one has to use the previously described tabular method evaluation system where the absolute evaluations for each criterion are shown.

Creating the graphical representation of data, we offer to put percent on X axis from 0 to 100 and on Y axis – 6 values of criteria. So using the bar diagram, where each method has its own color, a relative assessment is given to each method for every criterion. This axis division is desirable because it allows depicting and comparing several methods. So if the number of compared methods grows, the graphical diagram will increase vertically.

We consider that graphical representation as bar diagrams is only a recommendation and in every separate case the user can better appraise, which depiction scheme is more suitable for his needs. The system of evaluation and comparison states only criteria and calculable values of evaluations.

C. Classification of methods

The proposed evaluation system can be used not only for comparing methods, but also for classification of the methods. Criteria, in which it was necessary to choose from the different offered alternatives for evaluation of methods, are best suited for classification process. Criteria, in which the evaluations can adopt free values, such as SNR, are worse for classification purposes because they create a necessity to unify values in groups and such unifications would be mostly subjective. We think that the benefit of subjective classification is questionable and decided not to use this kind of classification.

We suggest using two criteria for the method classification: robustness versus data transmission forms and support of audio formats. The classification of methods according to created criteria will help the user of the system to choose the necessary methods, especially if he is intended to compare significant amount of methods. If the methods are classified before comparing and evaluating, the user will be able to select only those methods that can be used for his needs. Knowing the necessary characteristics of methods before will allow saving time (there is no need to define characteristic quantities for methods that are not suitable for users' purpose) as well as increase lucidity in both absolute and relative comparisons.

The classification gives chance not only to make the comparison more useful but also to arrange knowledge of steganographic methods storing their evaluation results. Within this paper an evaluation and comparison system as a software product is not created. But if a user stores these results in a database, the further described classification of methods can be used by getting and arranging data from the information storage.

The criterion that describes robustness versus signal transmission types is mentioned in Chapter II. We offer to create two-level classifications on its basis which is schematically presented in Figure 2.

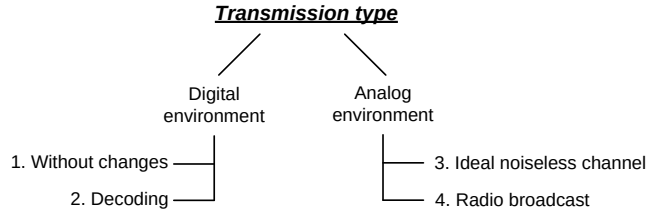

Fig. 2. Method classification according to transmission types

Differently from evaluation, the classification of the method has to be included in all corresponding categories. If any method suits the 3rd description (see Table I), it means that it can operate also with 1st and 2nd transmission type.

In classification process it means that the method is included in all classes which sequence number is smaller or the same as chosen sequence number during evaluation process by criterion *B* from Chapter II. This coherence is depicted in (12), where *m* is the method and *n* is chosen description sequence number by *T* criterion of method.

$$m \in [1, n] \quad (12)$$

For example, identifying method as "Transmission through the ideal noiseless analog channel" (according to Table I), it is automatically included in 1st, 2nd and 3rd class. First classes' level is intended to classification of the highest abstraction level (see Figure 2). We can see that transmission through the digital environment embraces steganographic audio methods of 1st and 2nd classes and transmission through the analog environment – 3rd and 4th classes. This classification is not compulsory but can be useful when working with a large number of methods.

The second classification type is based on supported audio formats that are described by criterion *F* in Chapter II and shown in Figure 2. The method will be presumed to the appropriate class, if it supports placing the message in definite audio format containers. So the criterion offers three classes: uncompressed audio, lossless compressed audio and lossy compressed audio.

IV. CONCLUSIONS

Unified evaluation system was developed with purpose to offer a possibility to evaluate and compare the steganographic

methods for processing of audio streams. The criteria of the system involve evaluation of methods from several points of view, basing upon the objective values and properties. The important feature of system is a unified branch of criteria which can be used for all audio steganographic methods. Each criterion method has a numerical assessment that allows not only evaluating the methods, but also comparing them by using only the proposed system and not looking on properties of each method.

Developing the system, we faced with difficulties, which are connected with classification of characteristic quantities. They had to separate quantities that describe methods in total from quantities that are specific for definite implementations. There was a research for summarized data that could be assigned to all methods by gathering data about evaluable methods in cases when results were connected with implementation.

The unified system of relative comparison of audio steganographic methods gives a chance to compare all methods one with another on the graphical diagram. With the fact that some evaluations do not have restricted values, it was not 100% possible to create a diagram according to maximal values and 100% was presumed result of best method acquired in each evaluation – that is why this comparing mode is relative against other methodic.

Populating the system's application area, the method classification possibilities were described by using the system criteria. But only two criteria were considered suitable for classification because they ensure the choice of evaluation from limited number of alternatives.

At this moment Unified Evaluation System is only a concept of methodology. But we plan to populate it's usage with developing of appropriate software product.

REFERENCES

[1] M.Wu, *Multimedia Data Hiding*. Princeton: Princeton University, Department of Electrical Engineering, 2001.

[2] B.Basile, K.Threlkeld, D.Valvano, *Surviving Attacks on Information Hiding and Audio Watermarking*, December 2008. [Online]. Available: http://cnx.org/content/m19003/1.1 [Accessed: Oct. 06, 2010].

[3] Don H. Johnson, *Signal-to-noise ratio*. Scholarpedia, 2006. [Online]. Available: http://www.scholarpedia.org/article/Signal-to-noise_ratio [Accessed: Sept. 30, 2010].

[4] I.J.Cox, M.L.Miller, J.A.Bloom, *Digital Watermarking and Steganography*. Morgan Kaufmann Publishers, 2008.

[5] P.Dutta, D.Bhattacharyya, T.Kim, *Data Hiding in Audio Signal: A Review*, "International Journal of Database Theory and Application", Vol. 2, 2009, pp. 1-8.

[6] *Free lossless audio codec.* [Online]. Available: http://flac.sourceforge.net [Accessed: Oct. 09, 2010].

[7] *The MPEG Home Page.* [Online]. Available: http://mpeg.chiariglione.org [Accessed: Oct. 09, 2010].

[8] D.Yan, R.Wang, *Huffman table swapping-based steganography for MP3 audio*, Multimedia Tools and Applications, Springer, 2009.

[9] G.Kipper, *Investigator's Guide to Steganography*. Washington D.C.: Auerbach Publications, 2004.

[10] D.Lavry. *Sampling Theory For Digital Audio*. Lavry Engineering, Inc., 2004.

Andrew Yershov, was born in 1984. Mg.sc.ing. (2008), B. sc. ing. (2005) – Riga Technical University (RTU), Institute of Applied Computer Systems.
IT project manager in the Latvian company "ABC software". Field of interests: computer science, data integration. Special interests: programming paradigms, distributed systems, Web technologies, steganography and steganalysis, cross-platform development, signal processing.

Roman Karpelcev, was born in 1988. B. sc. ing. (2010) – Riga Technical University (RTU), Institute of Applied Computer Systems.
Senior Programmer in Embedded Department in Accenture Riga Delivery Centre, Latvia. Participant in large scale embedded projects delivery. Previous experience includes computer network system administration and support in state institution. Field of interest: computer science. Special interests: embedded and system level software design and development, cross-platform development, networking technologies.

Andrejs Jeršovs, Romans Karpeļcevs. Vienotā vērtēšanas sistēma audio steganogrāfijas metodēm.
Ciparu steganogrāfija ir zinātne, kuras mērķis ir nodot paslēptu ziņojumu adresātam tā, lai ne tikai ziņojuma saturs, bet arī tā eksistences fakts paliktu nezināms. Pēc savas būtības tā ir jauna un vēl nepietiekami izpētīta zinātne, interese, kurai aug kopā ar multimediju datu izplatīšanu internetā. Strauji augoši multimediju datu apmaiņas apjomi rāda plašākas datu slēpšanas pielietošanas iespējas. Viens no ciparu steganogrāfijas virzieniem pēta informācijas slēpšanu audio plūsmās. Informācijas slēpšana audio plūsmās tiek uzskatīta par īpaši perspektīvu audio datu izplatīšanas un datu slēpšanas iespēju dēļ. Jau pastāv vairākas steganogrāfiskās metodes audio plūsmu apstrādei un pastāvīgi parādās jaunas metodes; tām ir atšķirīgas pielietošanas sfēras, īpatnības un izmantojamas slēpšanas tehnikas. Šajā rakstā tiek reprezentēta izstrādāta sistēma audio steganogrāfijas metožu vērtēšanai un salīdzināšanai. Izstrādāta sistēma dod iespēju efektīvi izvērtēt un salīdzināt gan esošas, gan nākotnē rādītas steganogrāfiskās metodes audio plūsmu apstrādei, izmantojot vienotu objektīvu kritēriju kopu. Šie kritēriji paredz metožu izvērtēšanu no vairākiem viedokļiem, balstoties uz objektīvajiem raksturojošiem lielumiem vai īpatnībām. Katrā kritērijā metode saņem skaitlisko vērtējumu, kas ļauj ne tikai izvērtēt metodes, bet arī salīdzināt tos savā starpā, izmantojot izveidotu sistēmu un neiedziļinoties katras metodes detalizētās īpašībās. Pēc metožu salīdzinājuma, kas tiek balstīts uz absolūtiem un relatīvajiem vērtējumiem, iegūtie rezultāti dod iespēju izvērtēt metožu priekšrocības / trūkumus un izvēlēties metodi atbilstoši izvirzītām lietotāja prasībām konkrētajā situācijā. Lai papildus palielinātu sistēmas izmantošanas iespējas rakstā tika aprakstītas metožu klasifikācijas iespējas, izmantojot iepriekš minētus sistēmas kritērijus. Neskatoties uz to, ka sistēma balstās uz sešiem kritērijiem, tikai divus no tiem autori uzskatīja par piemērotiem klasifikācijai, jo tikai tie nodrošina vērtējuma izvēli no ierobežotu variantu skaita.

Андрей Ершов, Роман Карпельцев. Единая система для оценивания методов аудио стеганографии.
Цифровая стеганография – наука, целью которой является передача скрытого сообщения адресату таким образом, чтобы не только содержание сообщения, но и его факт существования остался неизвестным. По существу, это новая и еще недостаточно изученная наука, интерес к которой растет вместе с распространением мультимедийных данных в Интернете. Стремительно растущие объемы обмена мультимедиа контентом создают широкие возможности для сокрытия данных. Одно из направлений цифровой стеганографии занимается исследованием методов скрытия информации в аудио потоках. Сокрытие данных в аудио потоках считается особенно перспективным из-за распространенности аудиоданных, а также из-за возможностей стеганографии при работе с ними. Уже существует множество стеганографических методов для обработки аудио; кроме того, постоянно появляются новые методы. У соответствующих методов разные сферы применения, характеристики и используемые техники сокрытия данных. В этой статье представлена разработанная система оценки и сравнения методов аудио стеганографии. Данная система дает возможность эффективно оценить и сравнить как существующие, так и разработанные в перспективе стеганографические методы для обработки аудио, используя единую объективную

систему критериев. Данные критерии подразумевают оценивание методов с разных точек зрения. По каждому критерию метод получает некое числовое значение, которое позволяет не только оценить методы, но также и сравнить их между собой, при этом, не вдаваясь в детали реализации. Полученная после применения системы сравнительная характеристика методов, которая основывается на абсолютных, а также относительных оценках, дает возможность оценить преимущества и недостатки каждого из сравниваемых методов. Таким образом, эти результаты позволяют эффективно выбрать методы аудио стеганографии, удовлетворяющие потребности пользователя в конкретной ситуации. Для расширения сферы применения системы статья также описывает возможности классификации, используя упомянутую систему критериев. Несмотря на то, что в основе системы лежат 6 критериев, только двое из них авторы рассматривают пригодными для классификации, так как они обеспечивают выбор оценки из неограниченного числа вариантов.