Scientific Journal of Riga Technical University
Computer Science. Applied Computer Systems
2010
Volume 43

Universal Stegoconstructor in Context of Intellectual Property Protection

Andrew Yershov, *Riga Technical University*, Pavel Rusakov, *Riga Technical University*

***Abstract* - Information interchange is one of the main processes in our everyday life. This process was simplified due to development of modern technologies, especially computer technologies. But the drawback of such transfer is the simplification of copyrights infringement. Steganography is modern science with old historical roots, its goal is during transmission to hide secret information. This science has some trends; in this case digital steganography is the most actual trend. One of digital steganography's research branches tries to find possible solutions of this problem. As a result of given researches the technologies of watermarks and fingerprints appeared. This paper contains information about the conception of digital steganography's development as protection method of the intellectual property. The basic scope of watermarking is classified, and the problem of selection of appropriate steganographic copyrights methods is designated. Eventually the universal constructor presented in the previous research is extended and adapted to resolve problem mentioned.**

Keywords: data protection, digital watermarking, fingerprinting, universal stegoconstructor, watermarking requirements

I. Introduction

The digital information revolution caused significant changes in the global society. Broadband communication networks and multimedia data available in a digital format (images, audio, video) opened many challenges and opportunities for innovations, but it also facilitates people to distribute large multimedia files and make their identical digital copies. Digital media files do not suffer from any quality loss due to multiple copying processes, such as analogue audio and VHS tapes. This advantage of digital media simultaneously transforms to the disadvantage, because a possibility for unlimited copying causes a considerable financial loss for copyright holders (basics of intellectual rights management). That is why the ease of content modification and quick distribution of illegal copies have promoted the protection of intellectual ownership [1], [2]. Traditional methods for copyright protection of multimedia data are no longer effective. Simple protection mechanisms were based on the information embedded into header bits of the digital file, but header information can easily be removed by a simple change of data format, which does not affect the fidelity of media [2].

In that case the achievements of the fast developing area of information hiding became especially useful – it is a question of digital steganography and watermarking. Steganography science researches the data hiding process from the "keeping the existence of the information secret" point of view, but watermarking – from "making the information imperceptible" point of view. Thereby digital watermarking is the technology for establishing ownership rights, tracking usage, ensuring authorized access, preventing illegal replications and facilitating content authentication [2].

This paper focuses on digital watermarking techniques. The authors describe the basics of digital watermarking systems, its area of use, introduce the problem of selection of the most appropriate method of watermarking protection for concrete data carrier or host signal and present the adapted universal stegoconstructor concept [3] to resolve the problem mentioned.

II. Steganography Usage in Intellectual Property Protection

Steganography is the science of hiding information in a way that its presence cannot be detected [4]. There are two kinds of information hiding scenarios:

- protection only against the detection of a message by a passive adversary and
- hiding a message with purpose to make impossible its removal even by an active adversary.

Steganography with a passive adversary was best illustrated by Simmons with "Prisoners' Problem" [5], [6]. Hiding information from active adversaries is a different problem since the existence of a hidden message is publicly known, such as in copyright protection schemes [1]. So the classification of this kind of steganography can be divided into 2 different classes:

1. Watermarking – marks digital objects with an identification of origin; all objects are marked in the same way.
2. Fingerprinting – identifies individual copies of an origin by embedding a unique marker in every copy that is distributed; if later an illegal copy is found, the copyright owner can identify the buyer by extracting the hidden information [6].

The watermarking and fingerprinting algorithms were primarily developed for digital images and video streams, as the result these data types have received most attention so far. Thus many methods of data hiding and intellectual properties protection have been developed, their effects are barely perceptible for humans, but can resist to distortions (noise) and tampering (security attacks) made by data transformations in communication channel that essentially conserve its contents.

III. Basics of Digital Watermarking

Digital watermarking is similar to watermarking physical objects except that the watermarking technique is used for digital content instead of physical objects [8]. Fig. 1 gives an overview of the general digital watermarking system [2].

A watermark represents a binary data sequence and is inserted into the data carrier (in general every signal can be considered as a carrier, because it can contain embedded information) in the **watermark encoder** or **embedder**. According to the logic of watermarking system, the watermark embedder has three inputs: watermark message, host signal or data carrier (for example: image, video clip or audio stream) and private watermark key (it is known only to authorized parties, so only these authorized parties can detect the watermark). The output of the watermark embedder is the watermarked signal, which cannot be perceptually distinguished from the host signal. Then watermarked signal is recorded on media carrier (CD, DVD) or distributed via broadcasting and later presented to the **watermark decoder** or **detector**. The detector attempts to determine watermark existence in the tested multimedia signal, and if so, what message is embedded in it.

Formally, a watermarking system can be described by a tuple (O, W, K, E_K, D_K, C_τ), where O is the set of all original data, W – the set of all watermarks, K – the set of all keys, E_K – the function of watermark encoder, D_K – the function of watermark decoder, C_τ – the comparator function, which verify the validity of detected watermark via decoding process. The two functions (1) and (2) represent the embedding and detection process [9]:

$$E_K : O \times W \times K \approx O \tag{1}$$

$$D_K : O \times K \approx W \tag{2}$$

The input parameters of the embedding process are the carrier object (or original host signal C_O), the watermark W to be embedded, as well as a secret or public key K. And the output of the encoder forms the marked dataset:

$$E_K(C_O, W) = C_W \tag{3}$$

In the detection process input parameters include the marked dataset C_W, the original C_O, the watermark W, and the key K used during the embedding process [9]:

$$D_K(C_W, C_O, W) = \hat{W} \tag{4}$$

On the output of the decoder extracted watermark $\hat{W}$ presents. Usually this watermark differs from the embedded watermark W due to possible manipulations. In order to validate the correspondence of both watermarks, the comparator function C_τ is used. This function compares the extracted watermark with the really embedded watermark using the threshold τ for comparison [9]:

$$C_\tau(\hat{W}, W) = \begin{cases} 1, C \geq \tau \\ 0, C < \tau \end{cases} \tag{5}$$

The threshold τ depends on the chosen algorithm, but it should be able to clearly identify the watermarks. The comparison result equals to 1 (true), if extracted watermark is valid, otherwise the result is 0 (false).

IV. Classification of Digital Watermarking Techniques

Digital watermarking techniques can be classified in various types. Each type mentioned below has different areas of use.

- *Robust and Fragile Watermarking* [8]. Robust watermarks are designed to resist against the data carrier distortions. It means that modification made to the watermarked content will not affect the watermark. This type of watermarks is required in secure watermarking systems. As opposed to this, fragile watermarks are embedded with very low robustness, i.e. watermark gets destroyed when watermarked content is modified or tampered with. These watermarks became useful in checking the integrity of objects.
- *Visible and Transparent Watermarking* [7]. Visible watermarks are embedded in visual content, that's why they are visible when the content is viewed. Transparent watermarks are imperceptible and can not be detected by just viewing the digital content.
- *Public and Private Watermarking* [9]. According to the basic principle of watermarking, the same key is used in the embedding and extracting/detecting processes. Thus, if the key is known, this type of watermark is considered as public, and if the key is hidden as private watermarks. In cases where security isn't a bottle neck of application, public watermarks are preferable, for example: metadata embedding.
- *Asymmetric and Symmetric Watermarking* [9]. Asymmetric watermarking (also called asymmetric key watermarking) is a technique where different keys are

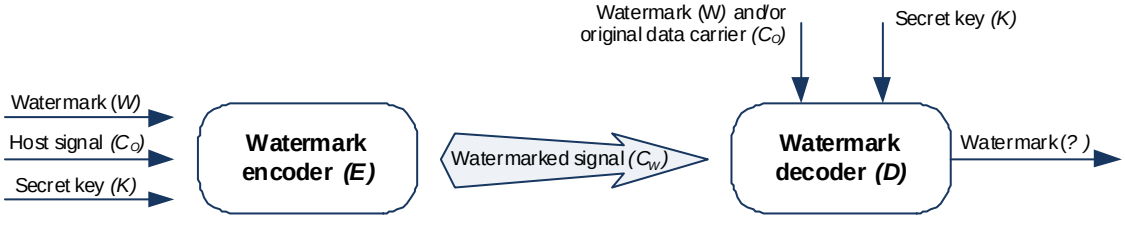

Fig. 1. General digital watermarking system

used for embedding and detecting the watermark. In symmetric watermarking (or symmetric key watermarking) the same keys are used for embedding and detecting watermarks.

V. Applications of Digital Watermarking

Digital watermarking becomes more important due to the development of global networks. The analysis of different information sources ([2], [8]) and researches of the literature ([9] – [11]) allow concluding that nowadays watermarking systems are widely used for the following objectives:

1. *Copyright or Ownership Protection*. Digital watermarks make it possible to identify and protect copyright ownership. In this case watermark containing ownership information is embedded in digital content. The embedded watermark has to be very robust and secure otherwise it can't survive processing modifications and intentional attacks in communication channel. On the other hand, ownership protection requires a small embedding capacity, because the number of bits that can be embedded and extracted with a small probability of error does not have to be large [2].
2. *Copy Protection or Access Control.* Digital content can be watermarked to indicate that the content cannot be illegally distributed. It means that the embedded watermark represents a certain copy control or access control policy. A watermark detector is usually integrated in a recording or playback system.
3. *Tracking or Fingerprinting* [8]. Digital watermarks can be used to track the usage of digital content. Each copy of digital content can be uniquely watermarked with metadata specifying the authorized users of the content. Such watermarks assist to detect illegal distribution of content by identifying the users who replicated the content illegally.
4. *Tamper Proofing* [8]. Digital content can be embedded with fragile watermarks that get destroyed whenever any distortion is made to the content. Usually such watermarks are intended for content authentication. In the content authentication applications, a secondary data is embedded in the host signal and later is used to determine whether the host signal was tampered. The robustness against removing the watermark is not a concern as there is no such motivation from attacker's point of view. However, forging a valid authentication watermark in an unauthorized or tampered host signal must be prevented.
5. *Broadcast Monitoring.* Digital watermarks can be used to monitor broadcasted content like television and broadcast radio signals. There are already available broadcast monitoring watermark-based applications on commercial basis, for example: program type identification, advertising research, broadcast coverage research etc. Users are able to receive the performance information that allows them to verify that the correct program and its associated promos are broadcasted as contracted and automatically track multimedia content using automated software online.
6. *Concealed Communication.* As digital watermarking is a kind of steganographic technique, it also can be used for concealed communication. The embedded watermark in this application is expected to have a high capacity.

VI. Optimized Watermarking Technique

Depending on the application, the digital watermarking techniques differ from each other. So the person, who is looking for the method of intellectual property protection via digital watermarking, usually encounters the problem of selection – "What kind of digital watermarking is better for appropriate host signal?" The problem is based on the absence of experience and uniform classification of digital watermarking techniques. As usual digital watermarking techniques are characterized with complexity of implementation and require additional time for learning, the person tries to find the similar solution and use it against searching for the optimized technique that is fully able to satisfy his requirements. Thus there is no opportunity to define the suitability of chosen method to customer's needs, if the comparative analysis of different similar methods is not done.

The authors of paper aim to divide the problem into two sub problems:

1. The unified classification of watermarking techniques.
2. The optimized technique selection.

The paper authors offer to classify watermarking techniques by requirements to watermarks and areas of use. The main watermarking requirements are robustness, invisibility, security, capacity and embedding/detection complexity [8]. Taking into account the described applications of digital watermarking, it is possible to evaluate the priority order of requirements presence (Table 1). The order of watermarking requirements is based on the usage logic of the every application and it was defined by the authors of this paper. It means that value in the appropriate table's cell represents the index place of requirement importance for concrete application. So any value must be used only once per application, and the most important requirement must have the highest priority (value "6").

In general, the dependence diagram of digital watermarking requirements can be constructed by averaging the value of every Table 1 column (Fig. 2). Averaging operation allows getting the priority order of watermarking requirements for optimized watermarking technique.

This diagram confirms that robustness and security are obligatory features of any watermarks. Besides mentioned above it corroborates the trade-offs of any data hiding techniques: "More robust $\rightarrow$ lower capacity", "lower invisibility $\rightarrow$ lower capacity" etc (Fig. 3).

On the one hand, this "Magic Triangle" ensures the classification of watermarking techniques by its usage sphere. But on the other hand it assists in selection of the appropriate technique by the watermark requirements. Unfortunately, it is useless if more than one watermark requirement are simultaneously defined. In other words, the problem of optimized technique selection arose.

TABLE 1

PRIORITY ORDER OF WATERMARKING REQUIREMENTS PER APPLICATION

	Embedding complexity	Detection complexity	Invisibility	Robustness	Security	Capacity
Copyright protection of media content carrier (CD, DVD)	2	3	4	6	5	1
Copy control of media content carrier (CD, DVD)	2	5	3	4	6	1
Concealed communication	1	3	6	5	2	4
Fingerprinting	2	4	3	5	6	1
Metadata addition to images/video	2	1	4	5	6	3
"Intelligent" broadcast	5	3	2	6	4	1
Average:	**2,33**	**3,17**	**3,67**	**5,17**	**4,83**	**1,83**

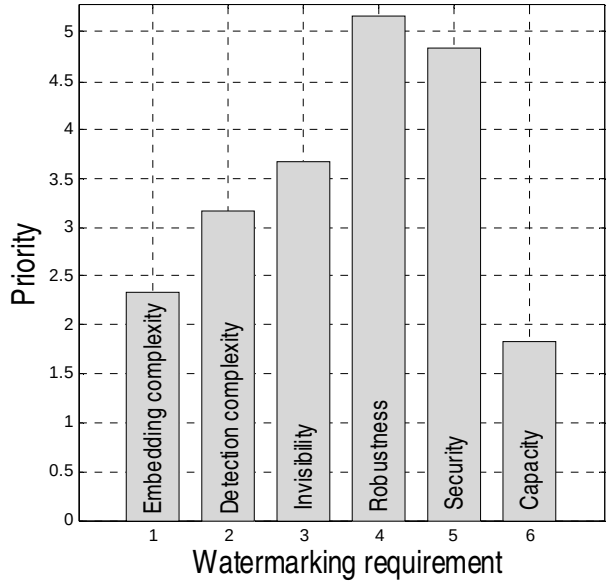

Fig. 2. Dependence diagram

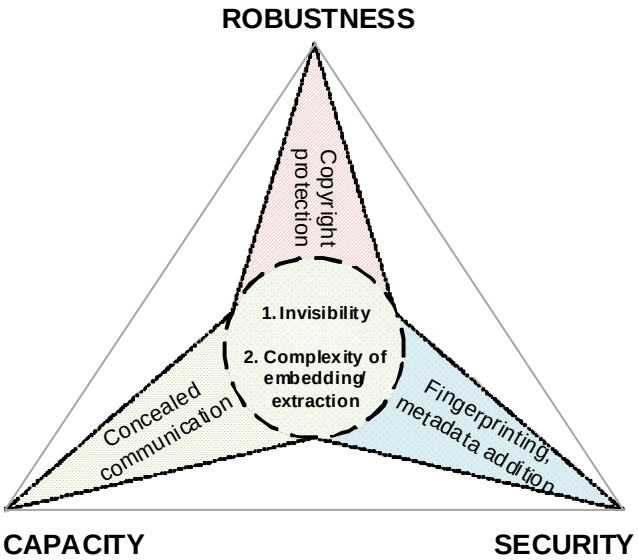

Fig. 3. "Magic Triangle" of watermarking techniques

VII. FINDING OPTIMIZED WATERMARKING TECHNIQUE

Finding the optimized watermarking technique is not an easy task. It demands additional human resources to make a comprehensive research and comparative analysis. That is why the usage of easing approaches systematizes the total process.

Authors of this paper developed the concept of universal stegoconstructor in their previous work [3], which allows receiving the most appropriate data hiding method for the chosen data carrier based on the given criteria [3]. As watermarking is special kind of data hiding, authors decided to adapt the stegoconstructor for finding/creating optimized watermarking technique.

Fig. 4 represents the adapted stegoconstructor that creates (or improves) necessary watermark embedding method according to the customer requirements. All steps of adapted stegoconstructor are described below.

On the *1st step* customer describes the application scope of needed intellectual property protection. During this step the requirements to watermark and watermarked data have to be defined with "Magic Triangle".

On the *2nd step* the algorithm is applied, which transforms host signal (or data carrier), taking into account format features chosen by the customer, so that methods of theory of signal transmission (TST) could be used comfortably [3], [12]. In this step also limitation list is created, which influences the selection of digital watermarking method in next steps.

The *3rd step* includes the analysis of received signal, taking into account the capacity requirements.

The *4th step* is the most important and complicated because in general it defines the features of optimized watermarking techniques. Moreover, before processing, methods of watermarked data should be used in this step, for example: encoding, compression, etc. Three possible ways of step's development exist:

- to choose/improve already existing digital watermarking method.
- to choose already existing TST method.
- to create a new method, taking into account the requirements of host signal.

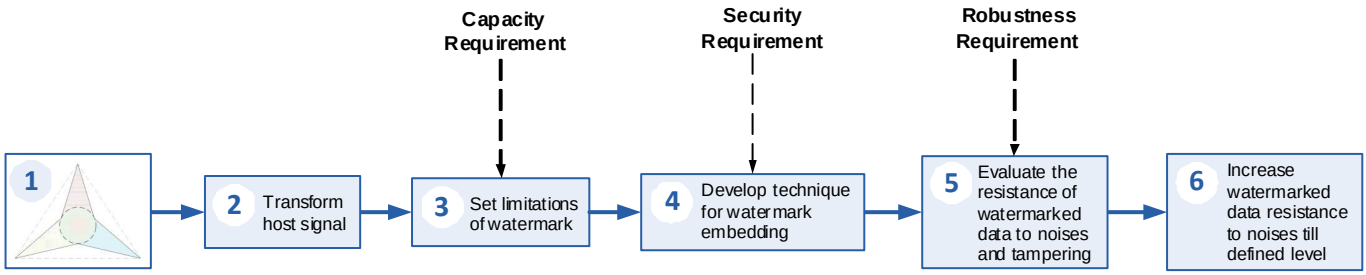

Fig. 4. Modified universal stegoconstructor

The result of fourth step is the algorithm of watermark embedding/detection in host signal.

The *5th step* evaluates the influence of transformations/ distortions on watermarked data. It means the conformance validation to required robustness level. If validation fails, then on the *6th step* imperfections of robustness is eliminated.

Comparing the adapted stegoconstructor concept with the original one, the following modifications were made:

1. The requirements of optimized technique are specified on the separate step using the developed "Magic Triangle" dependencies (the 1st step).
2. Two last steps of stegoconstructor became obligatory, because the main requirement of watermarks (robustness) is always set on it.
3. The step of developing the optimized technique is replenished with possibility to choose the existing watermarking method with purpose to upgrade it and make it suitable for defined needs.

VIII. Conclusions

In this paper achievements of digital watermarking in solving problems of intellectual property protection are described. Since digital watermarking is one of the main techniques in this section, there are discussed its main concepts and terminology.

The problem of choosing optimized watermarking method is revealed. That is why during this research there was an attempt to solve this problem. First of all, authors developed the classification method of watermarks by the priority order of features' requirements. The given classification forms the dependency of data hiding trade-offs between capacity, security and robustness. Secondly, the previously developed universal stegoconstructor was modified according to the mentioned dependency. Now every step of stegoconstructor is directed to fit the developed method to the customer needs of intellectual property protection. It means, that totally modified stegoconstructor ensures selection of the most suitable watermarking method.

References

[1] C. Cachin, "An information-theoretic model for steganography," in *Proceedings of 2nd Workshop on Information Hiding*. Springer, 1998.
[2] N. Cvejic, *Algorithms for Audio Watermarking and Steganography*. Finland: University of Oulu, 2004.
[3] A. Yershov and P. Rusakov, "Kutter steganographical method's improvement and concept of universal stegoconstructor," in *Scientific Proceedings of Riga Technical University*, Vol. 38. Riga: RTU, 2009, pp. 198-208.
[4] N. Provos and P. Honeyman, "Hide and seek: an introduction to steganography," *IEEE Security & Privacy Magazine*, vol. 1, no. 3, 2003, pp. 32-44.
[5] G. J. Simmons, "The prisoners' problem and the subliminal channel," in *Advances in Cryptology, Proceedings of CRYPTO '83*, 1984, pp. 51–67.
[6] A. Yershov and P. Rusakov, "The comparative analysis of digital steganographical methods LSB and Kutter," in *Scientific Proceedings of Riga Technical University*, Vol. 26. Riga: RTU, 2006, pp. 186-197.
[7] D. Milano, "Content control: digital watermarking and fingerprinting," White paper. [Online]. Available: http://rhozet.com/whitepapers/Fingerprinting_Watermarking.pdf. [Accessed: September 2009].
[8] "Digital watermarking: a technology overview," White paper. [Online]. Available: http://www.wipro.com/pdf_files/Digital_Watermarking_Tech_Overview.pdf. [Accessed: June 2009].
[9] M. Arnold, M. Schmucker, and S. D. Wolthusen, *Techniques and Applications of Digital Watermarking and Content Protection*. Boston: Artech House, 2003.
[10] P. Kanellis, E. Kiountouzis, and N. Kolokotronis, *Digital Crime and Forensic Science in Cyberspace*. London: Idea Group Publishing, 2006.
[11] N. Memon, *Information Hiding, Digital Watermarking and Steganography: An Introduction to Basic Concepts and Techniques*. Brooklyn: Polytechnic University, 2005.
[12] А. Б. Сергиенко, *Цифровая обработка сигналов*. Санкт-Петербург: Питер, 2003 (in Russian).

Andrew Yershov was born in 1984. He received bachelor degree in 2005 and master degree in 2008 from Institute of Applied Computer Systems, Riga Technical University.

He works as IT Project Manager in the Latvian company "ABC software". Field of interests: computer science. Special interests: programming paradigms, distributed systems, Web technologies, steganography and steganalysis.

Pavel Rusakov was born in 1972. he received master degree in 1995 and doctoral degree in 1998 from Riga Technical University.

He works as Associated Professor at the Institute of Applied Computer Systems, Riga Technical University. He is Head of Laboratory, responsible for the professional bachelor/master studies in Department of Applied Computer Science, Riga Technical University. Field of interests: computer science. Special interests: programming paradigms, parallel computing, Web technologies, distributed systems, computer graphics, protection of information.

Andrejs Jeršovs, Pāvels Rusakovs. Universālais stegokonstruktors intelektuālā īpašuma aizsardzības kontekstā
Informācijas apmaiņa ir viens no svarīgākiem procesiem cilvēka ikdienas dzīvē. Tā tika pavienkāršota, pateicoties modernu tehnoloģiju (īpaši informācijas tehnoloģiju) attīstībai. Bet tādas informācijas pārraides trūkums ir autortiesību pārkāpuma atvieglošana. Steganogrāfija – tā ir moderna zinātne ar garu vēsturi; tās mērķis ir slepenas informācijas pārraides fakta slēpšana. Eksistē šīs zinātnes dažādi virzieni; mūsdienās ciparu steganogrāfija kļūst par visaktuālāko virzienu. Viena no ciparu steganogrāfijas pētīšanas sfērām ir virzīta uz iepriekš minētas problēmas iespējamo risinājumu atrašanu. Tādēļ šo pētījumu rezultātā tika izveidota ūdenszīmju un pirkstu nospiedumu tehnoloģija. Šis raksts satur informāciju par ciparu steganogrāfijas attīstības koncepciju intelektuālā īpašuma aizsardzības metodes kontekstā. Izanalizēti ūdenszīmju tehnoloģijas pamati un nodefinēta piemērotas steganogrāfiskās metodes izvēles problēma autortiesību aizsardzībai. Rezultātā universālais stegokonstruktors, kurš tika izstrādāts iepriekšējā autoru izpētē, ir papildināts un adaptēts minētas problēmas risināšanai.

Андрей Ершов, Павел Русаков. Универсальный стегоконструктор в контексте защиты интеллектуальной собственности
Обмен информацией является одним из важнейших процессов в ежедневной жизни человека. Этот процесс упростился, благодаря развитию современных технологий, а особенно информационных технологий. Но недостатком подобной передачи информации является упрощение нарушения авторских прав. Стеганография – это современная наука со старыми историческими корнями; её цель – сокрытие факта передачи секретной информации. Существуют разные направления этой науки; в нашем случае цифровая стеганография представляет собой самое актуальное направление. Одна из ветвей исследований цифровой стеганографии занимается поиском возможных решений вышеописанной проблемы. Таким образом, в результате этих исследований и появилась технология водяных знаков вместе с отпечатками пальцев. Данная статья содержит информацию о концепции развития цифровой стеганографий в качестве метода защиты интеллектуальной собственности. Проанализированы основы технологии водяных знаков и определена проблема выбора наиболее подходящего стеганографического метода для защиты авторских прав. В итоге разработанный в прошлом исследовании авторов универсальный стегоконструктор был дополнен и адаптирован для решения упомянутой проблемы.