

# ОБНАРУЖЕНИЕ АУДИОСТЕГОСИГНАЛА С ВЛОЖЕНИЕМ ИНФОРМАЦИИ ПРИ ПОМОЩИ МОДУЛИРУЕМОЙ РЕВЕРБЕРАЦИИ

В.Г. Алексеев<sup>1</sup>, В.И. Коржик<sup>2\*</sup>

<sup>1</sup>ООО «Орион»,

Санкт-Петербург, 199406, Российская Федерация

<sup>2</sup>Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича,

Санкт-Петербург, 193232, Российская Федерация

\*Адрес для переписки: val-korzhih@yandex.ru

## Информация о статье

УДК 003.26

Язык статьи – русский

**Ссылка для цитирования:** Алексеев В.Г., Коржик В.И. Обнаружение аудиостегосигнала с вложением информации при помощи модулируемой реверберации // Труды учебных заведений связи. 2019. Т. 5. № 2. С. 102–107. DOI:10.31854/1813-324X-2019-5-2-102-107

**Аннотация:** Рассматривается аудиосигнал с вложением информации при помощи модуляции времени задержки реверберации. Хотя стегосистема такого вида обычно может использоваться для вложения цифровых водяных знаков, обеспечивающих защиту прав собственников аудиопродукции, но в некоторых случаях может представлять интерес обнаружение самого факта погружения дополнительной информации – то есть стегоанализ.

В работе показывается, что слуховое обнаружение, а также обнаружение по виду аудиосигнала оказывается невозможным при малых амплитудах вложения. Поэтому предлагается новый метод обнаружения, основанный на специфике реверберационной модуляции. Исследуется эффективность данного метода в обычных терминах стегоанализа (вероятность пропуска и ложного обнаружения стегосигнала).

**Ключевые слова:** стегосистема, реверберация аудиосигнала, стегоанализ, кепструм, корреляционный анализ.

## 1. Введение

Технология использования цифровых водяных знаков (ЦВЗ) является одним из наиболее эффективных методов обеспечения прав собственности на аудиопродукцию.

Действительно, если в некоторый аудиообъект предварительно произведено вложение информации, идентифицирующей его собственника, то впоследствии, если этот продукт оказывается нелегально выложенным, например, в Интернете или поступает в продажу через пиратские каналы, то собственник продукта, отследив при помощи мониторинга присутствие своего ЦВЗ, может обратиться в суд с целью возмещения убытков. Подобная практика широко рекламируется американской компанией Digimark, которая предлагает обслуживание для собственников аудиопродуктов.

Как правило, техника вложения ЦВЗ является открытой, т. е. любые пользователи могут обнаружить присутствие вложения и даже извлечь его. При разработке ЦВЗ ставится только задача обес-

печения стойкости относительно его удаления нелегитимным пользователем. Однако, в некоторых случаях подобную технику можно использовать и для скрытного вложения информации, тем более что она устойчива также и к такой относительно легкой атаке на стегосистемы, как «слепое удаление», когда стегоаналитик не может достоверно обнаружить присутствие стеганограммы (СГ), но пытается удалить возможные вложения без искажения аудиофайла. Поэтому может появиться задача обнаружения СГ в аудиофайлах, устойчивых к «слепому» удалению.

Известно несколько методов вложения ЦВЗ (или СГ) в аудиофайлы: вложение в наименьшие значащие биты (НЗБ), использование широкополосных сигналов (ШПС) [1], фазовая модуляция (ФМ) [2, 3], добавление эхо-сигналов (ЭС). Однако, НЗБ и ШПС приводят к заметным искажениям исходного аудиосигнала, т. е. покрывающего объекта (ПО), а методы ФМ и ЭС недостаточно устойчивы к удалению ЦВЗ даже без заметного искажения ПО.

Наиболее эффективным методом вложения ЦВЗ в аудиосигналы можно считать методы, основанные на модуляции реверберации. Один из таких методов описан и исследован в работе [5]. Настоящая статья посвящена методу обнаружения таких ЦВЗ, рассматриваемых как СГ. Она структурирована следующим образом: в разделе 2 описан метод вложения информации, предложенный в [5]. В разделе 3 предложен метод стегоанализа, пригодный для данной СГ. В разделе 4 эффективность такого метода исследована при помощи моделирования. Заключение суммирует основные результаты работы и формулирует перспективные, на наш взгляд, направления дальнейших исследований.

## 2. Описание метода вложения ЦВЗ в аудиофайлы, основанного на модуляции реверберации

Заметим, что, прежде всего, выбор метода реверберации для вложения не является случайным. Дело в том, что если производить модуляцию реверберации по задержке, т. е. на интервале вложения одного бита ЦВЗ использовать фильтры со сложной импульсной реакцией, но отличающиеся при вложении нуля и единицы только задержкой, то при выборе определенных параметров вложения (амплитуды, задержки и длительности битовых интервалов) это не приводит к заметному на слух искажению основного аудиосигнала.

Предположим, что ПО является файлом, содержащим цифровой аудиосигнал  $S(n)$ ,  $n = 1, 2, \dots, N$ , где  $N_0$  – объем файла в формате WAV на интервале вложения одного бита при скорости квантования сигнала 44,1 кГц и амплитудах отсчетов, представленных 16-ти битными последовательностями. Тогда, указанный выше метод вложения ЦВЗ может быть описан следующей формулой:

$$Z(n) = S(n) * h_b(n), \quad n = 1, 2, \dots, N, \quad b \in \{0, 1\}, \quad (1)$$

где  $Z(n)$  – сигнал после вложения;  $S(n)$  – аудиосигнал до вложения, называемый покрывающим объектом (ПО);  $h_b(n)$  – импульсная характеристика фильтра, зависящая от вкладываемого бита  $b$ ;  $*$  – операция свертки двух цифровых сигналов.

Для того, чтобы избежать искажений аудиосигналов, возникающих из-за переходных процессов между различными фильтрами, в работе [5] была использована «сглаживающая» функция. Как уже отмечалось ранее, импульсные реакции (ИР) фильтров, соответствующие вложению нуля  $h_0(n)$  и единицы  $h_1(n)$ , имеют сложную структуру, но отличаются только задержкой. Пример таких ИР показан на рисунке 1.

Применение комплексного кепстрального преобразования к обеим частям равенства (1) дает следующий результат [6]:

$$\tilde{Z}(n) = \tilde{S}(n) + \tilde{h}_b(n), \quad n = 1, 2, \dots, N, \quad b \in \{0, 1\}, \quad (2)$$

где « $\tilde{x}$ » означает кепстральное преобразование, соответствующее сигналу  $x(n)$ :

$$\tilde{x}(n) = \frac{1}{N} \sum_{k=0}^{N-1} \left( \log(x'(k)) + j\theta(k) \right) e^{\frac{2\pi jnk}{N}}, \quad (3)$$

где  $x'(k) = \sum_{k=0}^{N-1} x(n) e^{-\frac{2\pi jnk}{N}}$ ;  $x'(k)$  – амплитуда сигнала;  $\theta(k)$  – фаза сигнала;  $i = \sqrt{-1}$ .

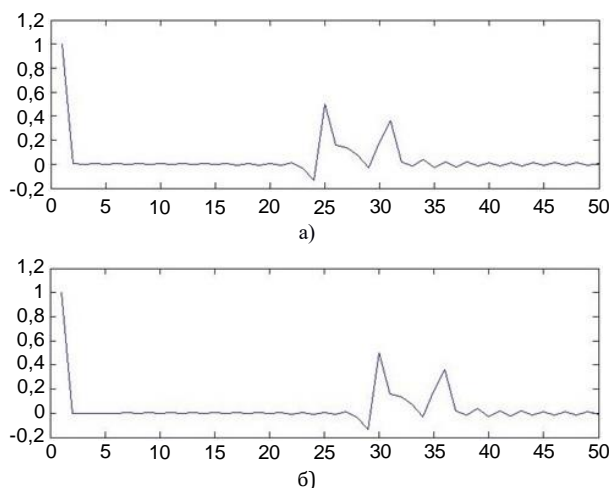


Рис. 1. Импульсная характеристика фильтров для бита «1» (а) и для бита «0» (б)

Преимущество кепстрального преобразования (2) перед представлением в виде свертки (1) состоит в том, что если  $\tilde{S}(n)$ ,  $n = 1, 2, \dots, N$ , можно аппроксимировать гауссовскими *i.i.d.*-величинами (от англ. Independent and Identically-Distributed), то оптимальный приемник, выделяющий бит  $b$  на каждом битовом интервале, будет иметь вид корреляционного приемника [5]:

$$b = \text{Arg}_{b \in \{0,1\}} \max \sum_{n=1}^{N_0} \tilde{Z}(n) \tilde{h}_b(n). \quad (4)$$

Если бы форма импульсной реакции  $h(n) = h_0(n)$ ,  $n = 1, 2, \dots, N_f$  была известна стегоаналитику, то, воспользовавшись правилом (4), он мог бы выделить вложенную информацию по данному правилу, как это делают легальные пользователи. В случае отсутствия шифрования информации для вкладываемых сообщений было бы возможно обнаружение СГ при выделении смысловых сообщений. Если бы собственник СГ (ЦВЗ) производил стойкое шифрование сообщений перед их вложением, то стегоаналитик мог бы использовать метод обнаружения СГ, основанный на NIST-тестах, описанный в работе [7]. Более того, стегоаналитик, даже в случае отсутствия уверенности в обнаружении СГ мог бы выполнить удаление этого вложения без искажения аудиосигнала, используя «обратные фильтры», метод построения которых подробно описан в [8].

Однако, если ИР  $h(n)$  является секретной функцией, и поэтому она неизвестна стегоаналитику,

то он не может применить упоминавшиеся выше методы стегоанализа. Конечно, предполагается, что для цифровых ИР  $h(n)$  количество их возможных вариантов должно быть непереборным. Заметим, что это условие не является слишком обременительным. Действительно, если типичная длина ИР соответствует «комнатному импульсу» [9], который сохраняет высокое качество аудиосигнала и равен примерно 180 отсчетам, то, предполагая, что амплитуда ИР соответствует примерно 20 % от максимальной амплитуды аудиосигнала, мы получим, что количество уровней квантования ИР будет примерно 13107, что приводит примерно к  $1,4 \cdot 10^{741}$  различным вариантам ИР [5] и является нереализуемым значением для атаки «прямого перебора».

Удаление вложения без заметного искажения аудиосигнала при неизвестной ИР  $h(n)$  так же оказывается невозможным, как это было показано в работе [5] при помощи введения дополнительных коротких импульсов в ИР фильтров. Разработка метода стегоанализа для описанной выше стегосистемы оказывается актуальной задачей.

### 3. Метод обнаружения СГ, использующей модуляцию реверберации по задержке

Идея обнаружения данной СГ основана на следующем свойстве сигналов после вложения: ИР, применяемые для вложения нулей и единиц, фильтров, отличаются только задержкой. Однако, расположение битовых интервалов, соответствующих вложенным нулям и единицам априори неизвестно. Если вложение не производилось, то в аудиосигнале может присутствовать отклик «комнатного импульса», но его модуляция по задержке будет отсутствовать.

Из данного свойства можно сделать следующие выводы, которые в дальнейшем будут использоваться для обнаружения данного вида СГ:

1) корреляция некоторого начального («эталонного») блока отсчетов кепструма на битовом интервале и какого-либо другого последующего блока на другом битовом интервале (при совпадении вложений на «эталонном» и текущем интервале) будет близка к единице;

2) отсутствует корреляция между кепструмами «эталонного» и текущего блока (если вложения на них не совпадают);

3) при равной вероятности нулей и единиц во вложении (при шифровании вложенных бит) вероятности 1-го и 2-го случая будут одинаковыми.

Казалось бы, можно определить наличие корреляции между блоками, сравнивая ее значения с некоторым заданным порогом:

$$R_3 = \sum_{n=1}^{N_0} \bar{Z}_3(n) \bar{Z}_T(n) \geq \lambda, \quad (5)$$

где  $\bar{Z}_3(n)$  – отчеты кепструма «эталонного» блока;  $\bar{Z}_T(n)$  – отчеты кепструма текущего блока;  $N_0$  – длина битового интервала;  $\lambda > 0$  – заданный порог.

Однако, выбор оптимального порога при вариативности уровня аудиосигнала оказывается весьма затруднительным. Потому в настоящей работе предложен метод обнаружения, основанный на количестве появления максимумов при введении (и невведении) задержки для отсчетов кепструма текущего и «эталонного» интервала:

$$R(b_3, b_T) = \sum_{n=1}^{N_0} \bar{Z}_3(n + b_3 N_3) \bar{Z}_T(n + b_T N_3), \quad (6)$$

где  $\bar{Z}_3()$  – отчеты кепструма сигнала на эталонном блоке;  $\bar{Z}_T()$  – отчеты кепструма сигнала на текущем блоке;  $b_3 = 0$ , если нет задержки на «эталонном» интервале;  $b_3 = 1$ , если введена задержка на «эталонном» интервале;  $b_T = 0$ , если нет задержки на текущем интервале;  $b_T = 1$ , если введена задержка на текущем интервале;  $N_3$  – величина задержки (в количестве отсчетов).

При этом мы исходим из весьма правдоподобной гипотезы, что  $R(b_3, b_T)$  по (6) для любого «эталонного» и текущего битовых интервалов при совпадающих символах вложения будут больше, чем аналогичные величины при несовпадающих символах.

В таблице 1 представлены возможные случаи появления максимумов корреляций  $R(b_3, b_T)$  в зависимости от состояния «эталонного» (ЭИ) и текущего (ТИ) битовых интервалов, а также вводимых (или нет) задержек на этих интервалах. Без потери общности предполагается, что при вложении «1» задержка ИР отсутствует, а при вложении «0» эта задержка присутствует.

Можно видеть, что отсутствие задержек для «эталонного» и текущего интервалов всегда приведет к тому же результату, что и наличие задержек для обоих интервалов, и потому достаточно рассмотреть только три варианта  $(b_3, b_T) = \{00, 01 \text{ и } 10\}$ .

Предполагая, что при наличии стойкого шифрования вложенной информации, когда вероятность вложения нулей и единиц одинакова, мы получим среднее количество максимумов в зависимости от состояния «эталонного» интервала и выбранных задержек на «эталонном» и текущем интервалах, которое представлено в таблице 2, где  $M$  – общее количество анализируемых битовых интервалов  $b$ .

Если же анализу подвергается аудиосигнал без вложения, то очевидно, что при выборе текущего интервала, достаточно удаленного от «эталонного», максимум функции (6) будет располагаться случайно и равновероятно, в зависимости от аргумента  $(b_3, b_T)$ , что и представлено в таблице 3. Также в этой таблице показаны средние значения количества максимумов (СКМ) в случае, когда анализируется аудиосигнал без модуляции по задержке

реверберационного фильтра (например, когда ИР-фильтры соответствуют «комнатному импульсу»).

ТАБЛИЦА 1. Наличие или отсутствие максимумов функции (6)

№	Состояние интервала		Введена (1), или нет (0) задержка		Наличие (+) или отсутствие (-) максимума
	ЭИ	ТИ	ЭИ	ТИ	
1	1	1	0	0	+
			0	1	-
			1	0	-
2	1	0	0	0	-
			0	1	-
			1	0	+
3	0	1	0	0	-
			0	1	+
			1	0	-
4	0	0	0	0	+
			0	1	-
			1	0	-

ТАБЛИЦА 2. Среднее количество максимумов функции (6) в зависимости от состояния ЭИ и вводимых задержек на ЭИ и ТИ

Вводимая задержка		СКМ	
$b_{\text{Э}}$	$b_{\text{Т}}$	«0» на ЭИ	«1» на ЭИ
0	0	$M/2$	$M/2$
0	1	0	$M/2$
1	0	$M/2$	0

ТАБЛИЦА 3. СКМ функции (6) в зависимости от задержек ( $b_{\text{Э}}, b_{\text{Т}}$ ) для аудиосигнала без вложения и аудиосигнала с реверберацией без модуляции

Вектор ( $b_{\text{Э}}, b_{\text{Т}}$ )	СКМ при отсутствии вложения	СКМ при наличии реверберации без модуляции
0 0	$M/3$	$M$
0 1	$M/3$	0
1 0	$M/3$	0

Наблюдая результаты, представленные в таблицах 1–3, можно предложить следующее логическое правило обнаружения рассматриваемой СГ, которое показано ниже:

$$\begin{aligned}
 & ((S(0, 0) \approx S(0, 1)) \cap (S(1, 0) \ll \\
 & \ll S(0, 1)) \cup (S(0, 0) \approx \\
 & \approx S(1, 0)) \cap (S(0, 1) \ll S(1, 0))),
 \end{aligned} \tag{7}$$

где  $S(i, j)$  – количество максимумов в зависимости от вектора ( $b_{\text{Э}}, b_{\text{Т}}$ ) = ( $i, j$ ); «U» – логическое «или»; «∩» – логическое «и».

Если правило (7) выполняется, то вложение присутствует, иначе – вложение отсутствует.

Поскольку условия, показанные в (7), являются «нечеткими», то в упрощенном варианте (т. е. не

вдаваясь в «теорию нечетких множеств»), можно для уточнения выбрать некоторые пороги  $\alpha, \beta$ , которые определяются экспериментально. Тогда правило решения о наличии или отсутствии СГ принимает следующий вид:

$$\begin{aligned}
 & ((|S(0, 0) - S(0, 1)| \leq \alpha) \cap (|S(1, 0) - S(0, 1)| \geq \beta)) \cup \\
 & (|S(0, 0) - S(1, 0)| \leq \alpha) \cap (|S(0, 1) - S(0, 1)| \geq \beta)).
 \end{aligned} \tag{8}$$

Если правило (8) выполняется, то вложение присутствует, иначе – вложение отсутствует.

Хотя из правила решения (8) видно, что для его использования придется предварительно выбрать пороговые значения, от которых мы в начале этой работы отказались. Однако ожидается, что эти пороги не окажутся весьма чувствительными к величине аудиосигнала и амплитуде вложения, потому что их экспериментальный выбор значительно упрощается.

#### 4. Экспериментальные исследования метода обнаружения стегосигнала

В таблице 4 приведены результаты экспериментального исследования функции (6) в зависимости от вектора аргумента ( $b_{\text{Э}}, b_{\text{Т}}$ ) для различных музыкальных композиций и вложения с модуляцией реверберации с различными амплитудами вложения.

ТАБЛИЦА 4. Средний процент присутствия максимумов функции (6) при различных векторных аргументах ( $b_{\text{Э}}, b_{\text{Т}}$ )

Музыкальная композиция	Амплитуда вложения	$(b_{\text{Э}}, b_{\text{Т}})$ , %		
		(0,0)	(0,1)	(1,0)
Mell, «Red Fraction»	Без вложения	33,5	35,5	31
	0,5	51	43,5	5,5
	0,3	48	43	9
О. Анофриев, «Есть только миг»	Без вложения	38,5	50	11,5
	0,5	53	36,5	10,5
	0,3	56	32	12
В. Высоцкий, «Песенка sentimentalного боксера»	41 %	35	24	41
	35 %	44	21	35
	34,5 %	46	19,5	34,5
Кипелов, «Я свободен»	Без вложения	37,5	40,5	30
	0,5	49	40,5	10,5
	0,3	50	46	4

Видно, что результаты эксперимента качественно соответствуют данным, представленным в таблице 2, хотя количественно они имеют значительный разброс, что объясняется случайной погрешностью и недостаточным объемом статистики.

В таблице 5 представлены результаты эксперимента для случая использования одного постоянного реверберационного фильтра без модуляции задержки с выбором различных «эталонных интервалов».



**ТАБЛИЦА 5. Средний процент максимумов при различных векторах аргумента ( $b_z$ ,  $b_T$ ) при использовании постоянного реверберационного фильтра**

Музыкальная композиция	Эталонный интервал	$(b_z, b_T)$ , %		
		(0,0)	(0,1)	(1,0)
Mell, «Red Fraction»	25	75	18	7
	35	83	3	14
О. Анофриев, «Есть только миг»	25	70	7	23
	35	60	21	19
В. Высоцкий, «Песенка сентиментального боксера»	25	38	3	59
	35	50	38	12
Кипелов, «Я свободен»	25	71	19	10
	35	73	10	17
Scorpions, «Still Loving You»	25	75	15	10
	35	69	13	18

Результаты таблицы 5 также качественно соответствуют данным таблицы 2. Для проверки эффективности алгоритма обнаружения были выбраны оптимальные значения  $\alpha$ ,  $\beta$  формулы (8) и проверено решение по этому правилу.

Количество музыкальных композиций было выбрано равным 20, хотя, конечно, этого недостаточно, чтобы получить надежные результаты. Однако по нему уже можно судить о работоспособности предложенного метода. Результаты эксперимента приведены в таблице 6.

#### Список используемых источников

1. Liu H., Zhang W. Overview of Audio Watermarking Algorithm against Synchronization Attacks // Proceedings of the International Conference on Artificial Intelligence: Technologies and Applications (ICAITA 2016). Advances in Intelligent Systems Research. Atlantis Press, 2016. PP. 210–213. DOI:10.2991/icaita-16.2016.52
2. Arnold M., Baum P.G., Voeßing W. A Phase Modulation Audio Watermarking Technique // Katzenbeisser S., Sadeghi A.R. (eds) Proceedings of the 11th International Workshop on Information Hiding (Darmstadt, Germany, 8–10 June 2009). Lecture Notes in Computer Science. Vol. 5806. Berlin: Springer, 2009. PP. 102–116. DOI:10.1007/978-3-642-04431-1\_8
3. Alekseyev V., Grudin A., Korzhik V. Design of Robust Audio Watermark System // Proceedings of the XI International Symposium on Problems of Redundancy in Information and Control Systems (Saint-Peterburg, Russia, 2-6 July 2007). St. Petersburg: Saint-Petersburg State University of Aerospace Instrumentation Publ., 2007. PP. 163–165.
4. Korzhik V., Morales-Luna G., Fedyanin I. Audio watermarking based on echo hiding with zero error probability // International Journal of Computer Science and Applications. 2013. Vol. 10. Iss. 1. PP. 1–10.
5. Korzhik V., Alekseev V., Morales-Luna G. Audio watermarking system resistant to removal attacks by dereverberation // International Journal of Computer Science and Applications. 2018. Vol. 15. Iss. 1. PP. 1–15.
6. Wu C.P., Su P.C., Kuo C.C.J. Robust Audio Watermarking for Copyright Protection // Advanced Signal Processing Algorithms, Architectures, and Implementations IX. Proceedings of International Symposium on Optical Science, Engineering, and Instrumentation (Denver, USA, 18–23 July 1999). SPIE. Digital Library, 1999. Vol. 3807. DOI:10.1117/12.367655
7. Korzhik V., Fedyanin I., Godlewski A., Morales-Luna G. Steganalysis Based on Statistical Properties of the Encrypted Messages // Computer Network Security. Proceedings of 7th International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security (MMM-ACNS, Warsaw, Poland, 28–30 August 2017). Lecture Notes in Computer Science. Cham: Springer, 2017. Vol. 10446. PP. 288–298. DOI:10.1007/978-3-319-65127-9\_23
8. Маркел Дж.Д., Грэй А.Х. Линейное предсказание речи. Москва: Связь, 1980. С. 45–46.
9. Arend J.M., Pörschmann C. Audio Watermarking of Binaural Room Impulse Responses // Proceedings of Audio Engineering Society International Conference on Headphone Technology (Aalborg, Denmark, 24–26 August 2016). AES E-LIBRARY, 2016. DOI:10.17743/aesconf.2016.978-1-942220-09-1

\* \* \*

**ТАБЛИЦА 6. Экспериментальные результаты по расчету вероятности пропуска СГ и вероятности ложного обнаружения**

Максимальная амплитуда вложения	Вероятности пропуска СГ ( $P_{пр}$ ), %	Вероятности ложного обнаружения ( $P_{лo}$ ), %
0,5	8	6
0,3	16	11

#### 5. Заключение

В статье предложен метод обнаружения перспективной системы ЦВЗ для аудиосигналов с модуляцией по задержке реверберационного фильтра. Поскольку непосредственное (слуховое) обнаружение вложенной таким способом СГ оказывается затруднительным, в частности, вследствие высококачественного вложения ЦВЗ, то решение задачи обнаружения предложенным в статье методом является весьма актуальным.

Эксперименты показали, что предложенный метод обнаружения СГ можно признать вполне работоспособным, хотя характеристики обнаружения и не являются идеальными. Впрочем, это обстоятельство может быть объяснено и тем фактором, что рассматриваемая система ЦВЗ оказалась достаточно устойчивой к обнаружению.

В дальнейшем представляется целесообразным уточнение и адаптация к амплитуде погружения порогов обнаружения  $\alpha$ ,  $\beta$ , используемых в алгоритме обнаружения, а также уточнение характеристик обнаружения при помощи увеличения объема ПО для проведения стегоанализа.

# DETECTING OF AUDIO STEGOSYSTEMS WITH INFORMATION EMBEDDING BASED ON MODULATED REVERBERATION

V. Alekseev<sup>1</sup>, V. Korzhik<sup>2</sup>

<sup>1</sup>Orion LTD,

St. Petersburg, 199406, Russian Federation

<sup>2</sup>The Bonch-Bruевич Saint-Petersburg State University of Telecommunications,

St. Petersburg, 193232, Russian Federation

## Article info

Article in Russian

**For citation:** Alekseev V., Korzhik V. Detecting of Audio Stegosystems with Information Embedding Based on Modulated Reverberation. *Proceedings of Telecommunication Universities*. 2019;5(2):102–107. (in Russ.) Available from: <https://doi.org/10.31854/1813-324X-2019-5-2-102-107>

**Abstract:** Audio signal with embedding of information based on modulated reverberation is considered. The goal of such stegosystem commonly is to provide a copy right protection by digital watermarking but sometimes may be interesting also to detect a fact of hidden signal presence by means of steganalysis. Detecting of such stegosystems occurs impossibly when it is executed either by a listening of audio signal or by a observation of signal wave form if depth of embedding is very small. Therefore we propose a new detection algorithm based on properties of modulated reverberation. A performance evaluation of such algorithm is investigated by simulation in terms of the probability of missing and the probability of false alarm.

**Keywords:** stegosystem, reverberation of audio signal, steganalysis, cepstrum, correlation analysis.

## References

1. Liu H., Zhang W. Overview of Audio Watermarking Algorithm against Synchronization Attacks. *Proceedings of the International Conference on Artificial Intelligence: Technologies and Applications (ICAITA 2016)*. Advances in Intelligent Systems Research. Atlantis Press; 2016. p.210–213. Available from: <https://doi.org/10.2991/icaita-16.2016.52>
2. Arnold M., Baum P.G., Voeßing W. A Phase Modulation Audio Watermarking Technique. In: Katzenbeisser S., Sadeghi A.R. (eds) *Proceedings of the 11th International Workshop on Information Hiding, 8–10 June 2009, Darmstadt, Germany*. Lecture Notes in Computer Science. Vol. 5806. Berlin: Springer; 2009. p.102–116. Available from: [https://doi.org/10.1007/978-3-642-04431-1\\_8](https://doi.org/10.1007/978-3-642-04431-1_8)
3. Alekseyev V., Grudin A., Korzhik V. Design of Robust Audio Watermark System. *Proceedings of the XI International Symposium on Problems of Redundancy in Information and Control Systems, 2–6 July 2007, Saint-Peterburg, Russia*. St. Petersburg: Saint-Petersburg State University of Aerospace Instrumentation Publ.; 2007. p.163–165.
4. Korzhik V., Morales-Luna G, Fedyanin I. Audio watermarking based on echo hiding with zero error probability. *International Journal of Computer Science and Applications*. 2013;10(1):1–10.
5. Korzhik V., Alekseev V., Morales-Luna G. Audio watermarking system resistant to removal attacks by dereverberation. *International Journal of Computer Science and Applications*. 2018;15(1):1–15.
6. Wu C.P., Su P.C., Kuo C.C.J. Robust Audio Watermarking for Copyright Protection. *Advanced Signal Processing Algorithms, Architectures, and Implementations IX. Proceedings of International Symposium on Optical Science, Engineering, and Instrumentation, 18–23 July 1999, Denver, USA*. SPIE. Digital Library; 1999. Vol. 3807. Available from: <https://doi.org/10.1117/12.367655>
7. Korzhik V., Fedyanin I., Godlewski A., Morales-Luna G. Steganalysis Based on Statistical Properties of the Encrypted Messages. *Computer Network Security. Proceedings of 7th International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security (MMM-ACNS), 28–30 August 2017, Warsaw, Poland*. Lecture Notes in Computer Science. Cham: Springer, 2017. Vol. 10446. p.288–298. Available from: [https://doi.org/10.1007/978-3-319-65127-9\\_23](https://doi.org/10.1007/978-3-319-65127-9_23)
8. Markel D.D., Grei A.K. *Lineinoe predskazanie rechi* [Linear Speech Prediction]. Moscow: Sviaz Publ.; 1980. p.45–46. (in Russ.)
9. Arend J.M., Pörschmann C. Audio Watermarking of Binaural Room Impulse Responses. *Proceedings of Audio Engineering Society International Conference on Headphone Technology, Aalborg, Denmark, 24–26 August 2016*. AES E-LIBRARY; 2016. Available from: <https://doi.org/10.17743/aesconf.2016.978-1-942220-09-1>