УДК 004.056.5

СТЕГАНОГРАФИЧЕСКИЙ АЛГОРИТМ СКРЫТИЯ ДАННЫХ В ЧАСТОТНОЙ ОБЛАСТИ АУДИОСИГНАЛОВ, УСТОЙЧИВЫЙ К СЖАТИЮ

Н. В. Калашников, А. А. Яковенко, Н. И. Кушниренко

Одесский национальный политехнический университет
Украина, г. Одесса
kalashnikov_n.v@ukr.net

Разработан новый метод стеганографического скрытия данных в частотной области аудиосигнала со сжатием без потерь с использованием быстрого преобразования Уолша—Адамара. В качестве контейнера рассматривается аудиофайл формата FLAC, скрытие информации осуществляется в остаточном сигнале.

Ключевые слова: стеганография, скрытие данных, частотная область, быстрое преобразование Уолша—Адамара.

Стеганографические методы основаны на модификации цифровых контейнеров без нарушения целостность восприятия последних с целью незаметного и надежного сокрытия битовых последовательностей — стеганосообщений (СС) [1]. Остается актуальным поиск новых стеганографических алгоритмов (СА).

Наиболее часто для скрытия информации в частотной области аудиосигнала применяется дискретное преобразование Фурье [2]. Поскольку данное преобразование требует значительных объемов вычислений, будет оправданным использование более простых и быстрых алгоритмов, например преобразования Уолша—Адамара [3], в виде быстрого преобразования Уолша—Адамара (БПУА).

Для оценки качества стегосистемы определяются некоторые параметры вносимых искажений при скрытии СС в стеганоконтейнере (СК), пропускная способность стегоканала, устойчивость данных при сжатии и искажениях [4].

Цель работы — разработка нового СА для сокрытия данных в аудиофайле (АФ) формата FLAC.

В данной работе были решены следующие задачи.

1. Произведен анализ структуры АФ формата FLAC с целью выявления элементов, пригодных для скрытия данных.

2. Определены критерии оценки эффективности работы СА для АФ.

3. Разработан СА для скрытия данных в частотной области остаточного сигнала (ОС) АФ формата FLAC.

В качестве СС рассматривается битовая последовательность $p_1,p_2,...,p_t$ где $p_i \in \{0, 1\}$, $i = 1,2,...,t$. В качестве секретных ключей для декодирования СС используются значение уровня сжатия C и номера используемых коэффициентов БПУА m, n. Пропускная способность стегоканала составляет $R = N/8$, где N – частота дискретизации для данного СК. Тестирование алгоритма производится путем моделирования его работы в среде Matlab. В данной работе для создания АФ формата FLAC применяется утилита FLAC-Frontend 2.0 с уровнем сжатия $C = 5$. Запись осуществляется в остаточный сигнал одного аудиофрейма АФ. Длины битовой последовательности $t_1 = 200$, $t_2 = 500$. Значение порога распознавания $P = 6$. Работа алгоритма осуществляется следующим образом.

Шаг 1. Считывается ОС каждого аудиофрейма АФ. Выбираются значения порога распознавания P , номера используемых коэффициентов БПУА.

Шаг 2. Осуществляется запись СС. R — ОС одного аудиофрейма, p_i — очередной бит СС.

2.2. Производится БПУА ОС: $X(k) = БПУА(R)$, где k — функции Уолша.

2.3. Массив коэффициентов БПУА X разбивается на блоки 1×8 $Xj = (X_{1,j}, X_{2,j}, ...,X_{8,j})$.

2.4. Если $p_i=0$, то $X_{m,j}$ корректируется таким образом, чтобы выполнялось условие

$|X_{m,j}| - |X_{n,j}| > P$; иначе — корректируется $X_{n,j}$ так, чтобы $|X_{m,j}| - |X_{n,j}| < -P$. В результате происходит искажение коэффициентов БПУА $X_{m,j}$, если p_i=0 или $X_{m,j}$, если p_i=1.

Шаг 3. Производится сборка массива измененных коэффициентов БПУА, выполняется обратное БПУА ОС: $R' = ОБПУА(X(k))$.

Шаг 4. Производится запись измененного ОС в АФ, корректируются значения контрольных сумм аудиофреймов и хэш-суммы несжатого аудиосигнала в АФ.

Алгоритм для декодирования СС выглядит следующим образом.

Шаг 1. Считывается ОС каждого аудиофрейма АФ.

Шаг 2. Осуществляется считывание СС. R — ОС одного аудиофрейма, p_i — очередной бит СС.

2.2. Производится БПУА ОС: $X(k) = БПУА(R)$.

2.3. Массив коэффициентов БПУА разбивается на блоки 1×8 $X_j = (X_{1,j}, X_{2,j}, ..., X_{8,j})$.

2.4. Если $|X_{m,j}| > |X_{n,j}|$, то p_i=0; иначе — p_i=1.

Результаты лабораторного тестирования приведены в таблице.

Зависимость искажений СК от длины СС

Название показателя искажения	Значение при t = 200	Значение при t = 500
Максимальная разность, MD	774	1197
Средняя максимальная разность, AD	167,3125	274,537
Нормированная средняя максимальная разность, nAD	0.2020	0,331
Среднеквадратичная ошибка, MSE	$4.526 \cdot 10^4$	$1{,}217 \cdot 10^5$
Нормированная среднеквадратичная ошибка, NMSE	0,0087	0,023
Отношение «сигнал/шум», SNR	115,4617	42,935
Максимальное отношение «сигнал/шум», PNSR	$1{,}189 \cdot 10^4$	$4{,}421 \cdot 10^3$
Нормированная взаимная корелляция, NC	1,001	1,011
Структурное содержание, SC	0,991	0,958

Таким образом, в результате проведенного анализа структуры АФ формата FLAC установлено, что оптимальным является использование ОС АФ, созданного при значении уровня сжатия C = 3...5. При этом обеспечивается полная устойчивость СК к сжатию с использованием алгоритма сжатия FLAC, поскольку при известном получателю СС значении C возможно восстановление СК без искажений. Предложенный стеганографический метод для скрытия данных в АФ формата FLAC обладает незначительными вносимыми искажениями в СК, практически не различимыми для слуховой системы человека.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Грибунин В. Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. — Москва: Солон-пресс, 2002.

2. Залманзон Л. А. Преобразования Фурье, Уолша, Хаара и их применение в управлении, связи и других областях. — Москва: Наука, 1989.

3. Айфичер Э. С., Барри У. Д. Цифровая обработка сигналов. — Москва: Вильямс, 2004.

4. Конахович Г. Ф., Пузыренко А.Ю. Компьютерная стеганография. — Киев: МК-Пресс, 2006.

N. V. Kalashnikov, A. A. Iakovenko, N. I. Kushnirenko

Compressive-stable steganographic algorithm for data hiding in the frequency domain of audio signals.

A new steganographic method is developed for data hiding in the frequency domain of an audio signal with lossless compression using a fast Walsh-Hadamard transform. The structure of the FLAC file format is analyzed in order to identify the elements that are suitable for data hiding. An audio data in FLAC is considered as a container, data hiding is performed in the residual signal.

Keywords: *steganography, data hiding, frequency domain, fast Walsh-Hadamard transform.*