

05, май 2016

УДК 004.357

Исследования применимости метода LSB для сокрытия текстовой и графической документации в аудиосреде

*Козарь А.А., студент
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Робототехника и комплексная автоматизация»*

*Научный руководитель: Волосатова Т.М., к.т.н., доцент
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Робототехника и комплексная автоматизация»
tanaravol@bmstu.ru*

Введение

Защита от несанкционированного доступа проектной документации, продуцируемой в средах CAD/CAM/PDM/PLM с применением CALS – технологий является актуальной задачей, решение которой осуществимо двумя группами методов:

- Криптографические.
- Стеганографические.

Факт защиты данных криптографическими методами скрыть невозможно и это упрощает криптоанализ. Кроме того эти методы сложны в реализации. Поэтому они чаще всего применяются для кодирования данных, составляющих государственную тайну. Для сохранения коммерческой тайны и исключения возможности занесения ложных данных разумнее применение стеганографических данных. Кроме того стегосообщения можно передавать по открытым каналам.

При этом по каналу связи передаются уже не сами защищаемые данные, а результат их встраивания в контейнер, и для противника возникает сложная задача вскрытия шифра [1, с. 11]. Как известно [3, с. 196], наиболее просто реализуется стеганографический метод LSB, но он характеризуется значительной ограниченностью допустимого объема стего при сокрытии в контейнерах – изображениях (до 8%). Именно применение аудиофайла в качестве контейнера расширяет возможности применения этого метода для защиты проектной документации от несанкционированного доступа. При поведении исследований ставилась задача найти сочетание простоты реализации метода с возможностью сокрытия проектной документации. Аналитический обзор доступной

литературы показал [1-4], что исследования в области возможностей применения аудиофайлов в качестве контейнеров, заполняемых методом LSB проведены не в полной мере.

1. Цель и задачи исследований

Целью исследований, основные результаты которых приведены далее, является определение криптоустойчивости LSB – стегокодирования в аудиофайлах проектной документации с учетом возможных помех в каналах связи [6]. Под проектной документацией понимались чертежи, электрические схемы, спецификации и тексты программ, которые необходимо передать по открытым каналам для проведения необходимых доработок сопровождаемого объекта проектирования. Для достижения поставленной цели решены следующие задачи:

- разработка программного средства для проведения численных экспериментов.
- конвертирование графических файлов к виду, удобному для занесения в аудиоконтейнер.
- определение криптоустойчивости реализаций метода при воздействии аддитивного коррелированного шума на стегосообщение.
- определение предельного объема стего с помощью сопоставительного анализа осциллограмм и спектров пустого контейнера и контейнера со стего.

Соккрытие данных в аудиосигналах является особенно интересным для исследования, поскольку слуховая система человека (ССЧ) работает в сверхшироком динамическом диапазоне и, кроме того, является чувствительной к белому шуму. Отклонения в звуковом файле могут быть выявлены вплоть до одной десятимиллионной (на 70 дБ ниже уровня внешних шумов) [3, с. 196].

2. Описание программной реализации метода. Интерфейс программной среды.

Запуск приложения вызывает главное окно программы (рис. 1).

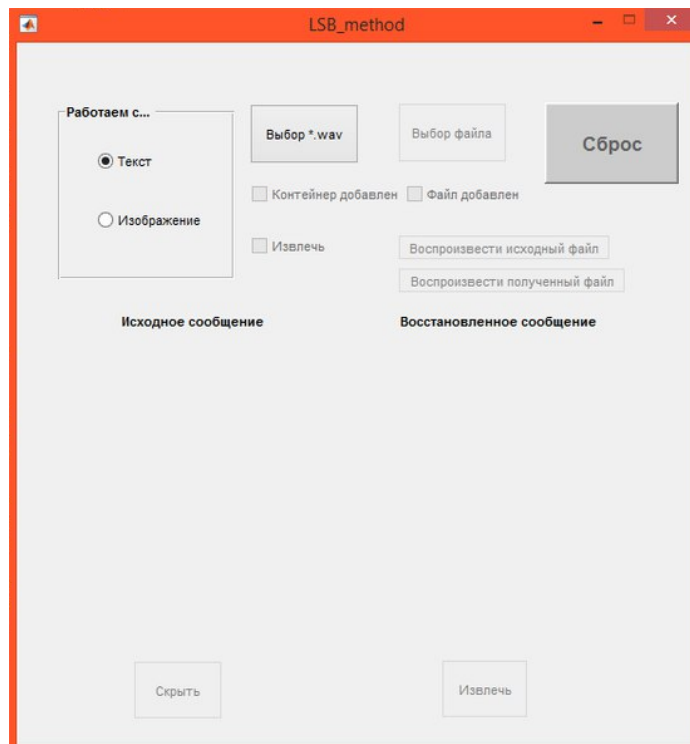


Рис. 1. Главное окно интерфейса

С его помощью пользователь осуществляет работу с файлами. Предоставляется возможность выбора формата скрываемой информации (графическая или текстовая), а также выбора аудиоконтейнера. В поле «Исходное сообщение» на экран выводится содержимое скрываемого файла. После выбора контейнера и файла для сокрытия, появляется возможность нажатия на кнопку «Скрыть», что приведет к встраиванию сообщения в аудиоконтейнер. После появления сообщения об успешности сокрытия, пользователь может выбрать заполненный аудиоконтейнер и извлечь сообщение, которое будет выведено на экран в поле «Восстановленное сообщение».

Программное средство реализовано в программной GUI Matlab.

3. Основные результаты численного эксперимента

Количество кодируемых младших бит может варьироваться в зависимости от ситуации [4]. Сравним искажения аудиоконтейнера при различном количестве заменяемых бит.

На рис. 2а-2б представлено распределение амплитуд пустого контейнера-сигнала длительностью 3 сек и аудиоконтейнера, заполненного текстовой информацией (500 символов) с кодированием двух бит. Рис. 2в представляет разность амплитуд

заполненного контейнера, содержащего скрытое сообщение, и пустого контейнера. Проведем анализ соответствующих данных.

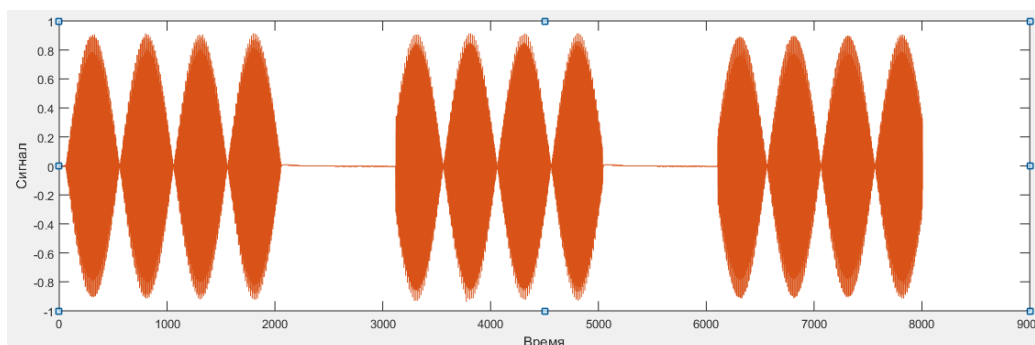


Рис. 2а. Пустой контейнер

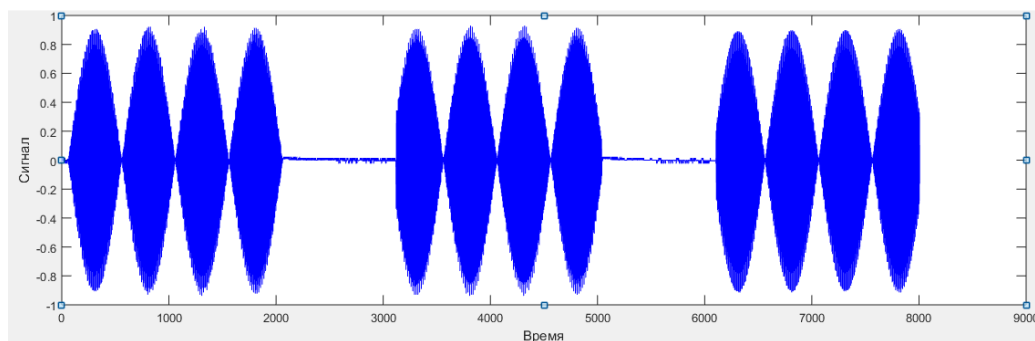


Рис. 2б. Заполненный контейнер (2 бита)

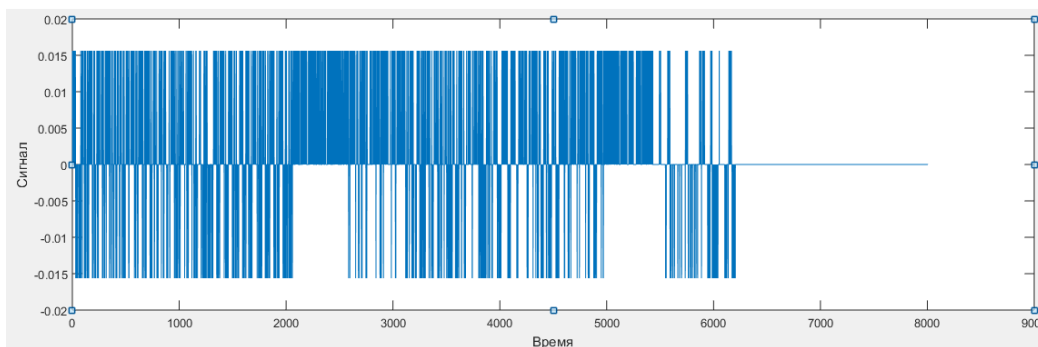


Рис. 2в. Разность амплитуд заполненного (2 бита) и пустого контейнера

Можно заметить небольшое искажение, вызванное заменой двух бит. Однако величина разности амплитуд по сравнению с амплитудами заполненного и пустого контейнера незначительна.

Увеличим количество бит до четырех (рис. 3а -3в).

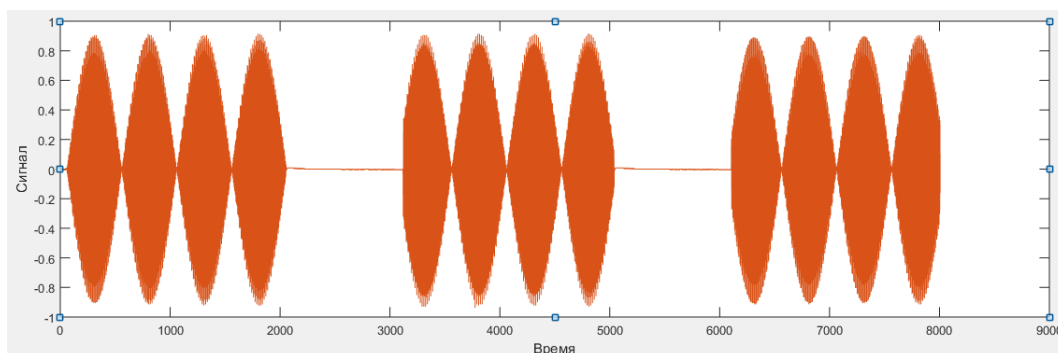


Рис. 3а. Пустой контейнер

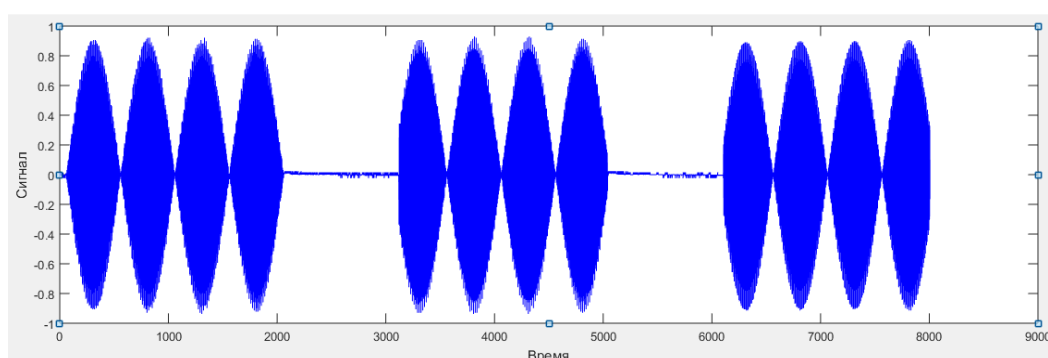


Рис. 3б. Заполненный контейнер (4 бита)

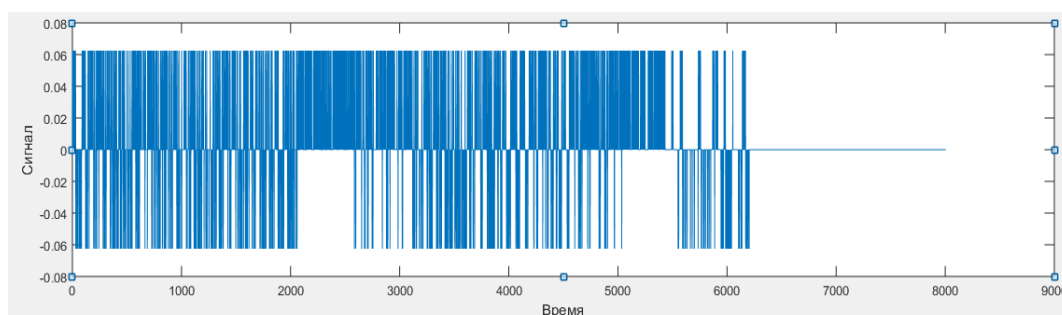


Рис. 3в. Разность амплитуд заполненного (4 бита) и пустого контейнера

Несмотря на то, что при оценке контейнеров на слух, для среднестатистического слушателя разница была практически не заметна, на графиках можно отметить более значительное искажение исходного контейнера. На графике разности амплитуд можно также заметить увеличение искажений. Из графика разности амплитуд также можно сделать вывод о занимаемом скрытым сообщением пространстве в контейнере.

Проведен соответствующий эксперимент, используя аудиоконтейнер большей длительности (1 минута 36 секунд) и более сложной структуры. Рассмотрено кодирование 2 бит (рис. 4а-4в) и кодирование 4 бит (рис. 5а-5в).

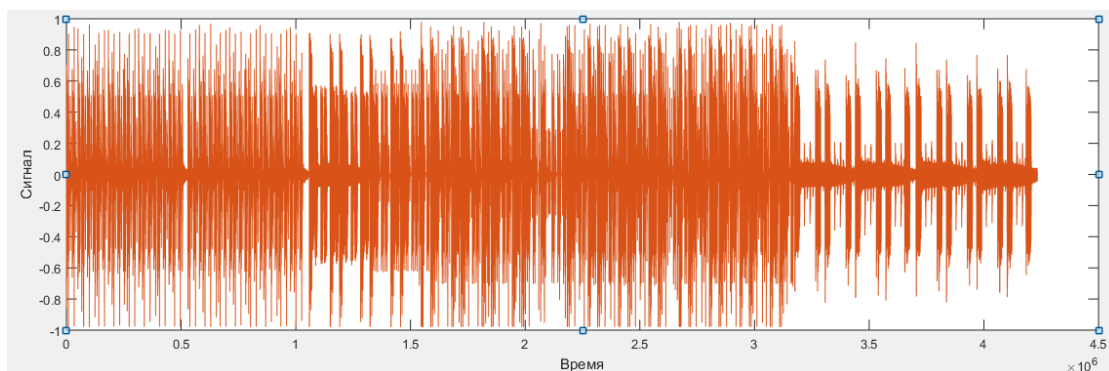


Рис. 4а. Пустой контейнер

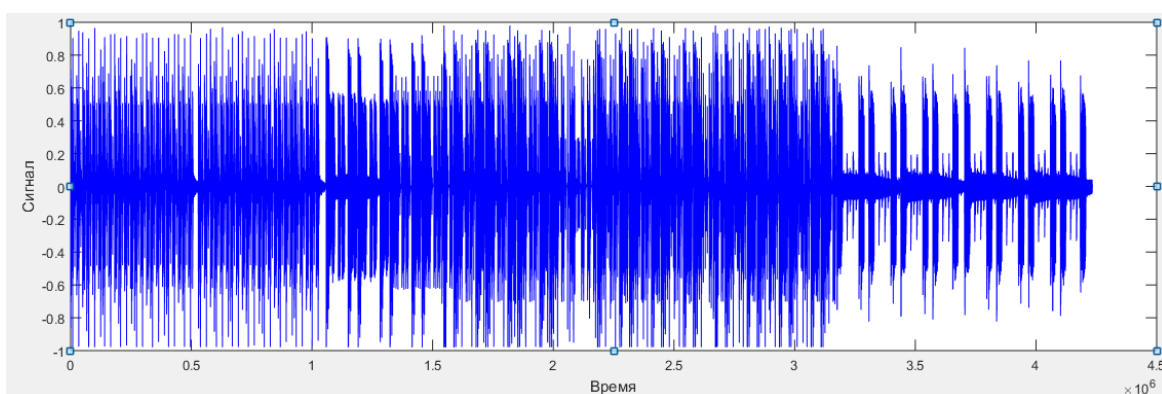


Рис. 4б. Заполненный контейнер (2 бита)

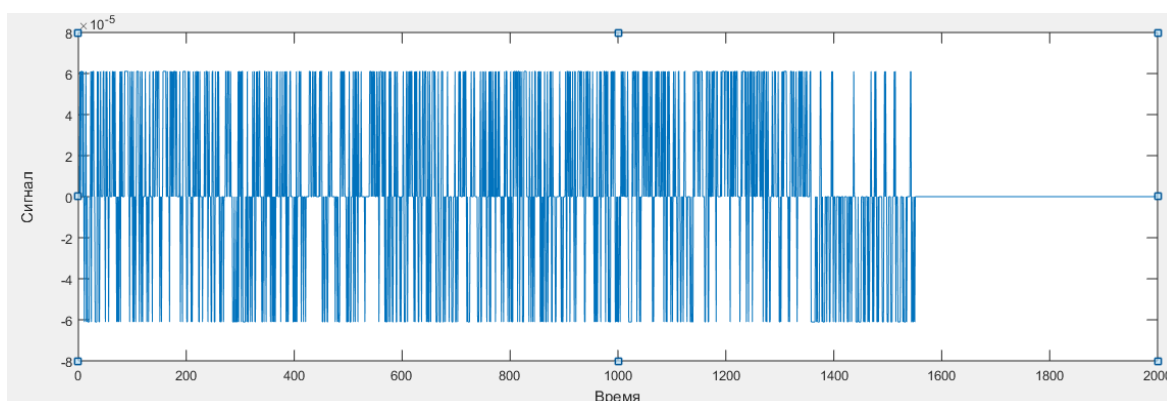


Рис. 4в. Разность амплитуд заполненного (2 бита) и пустого контейнера

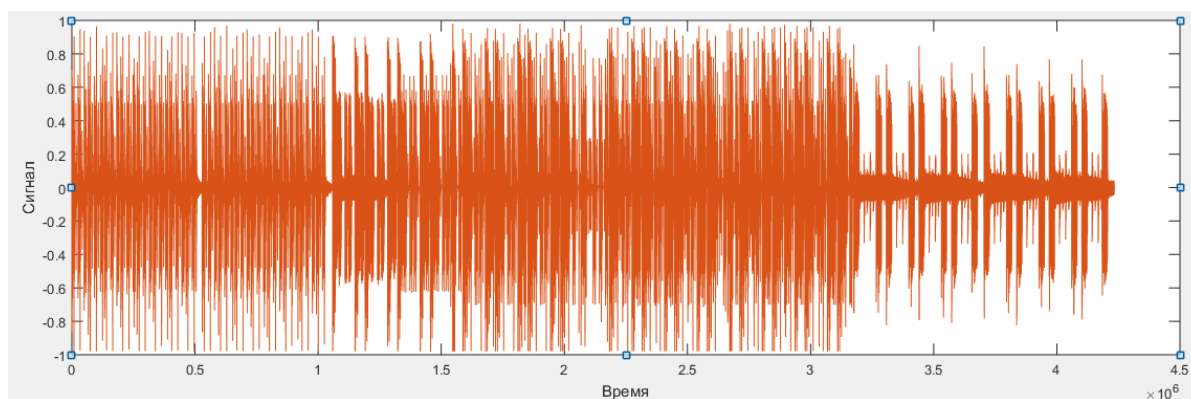


Рис. 5а. Пустой контейнер

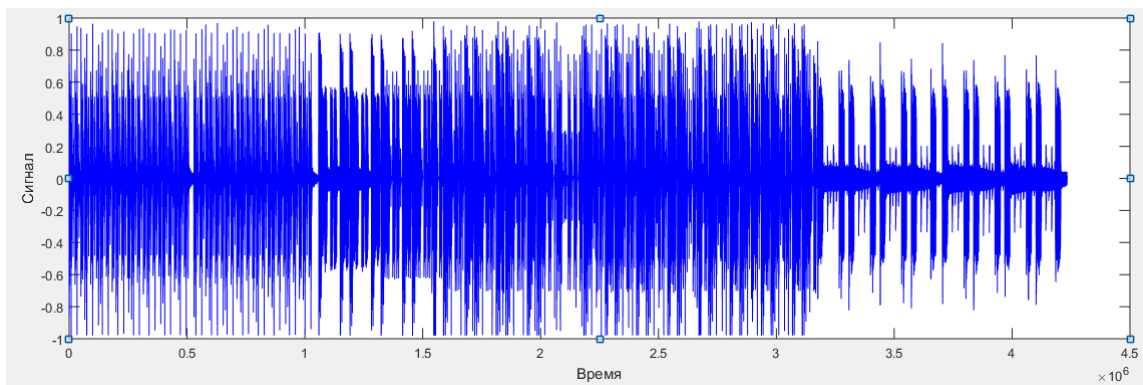


Рис. 5б. Заполненный контейнер (4 бита)

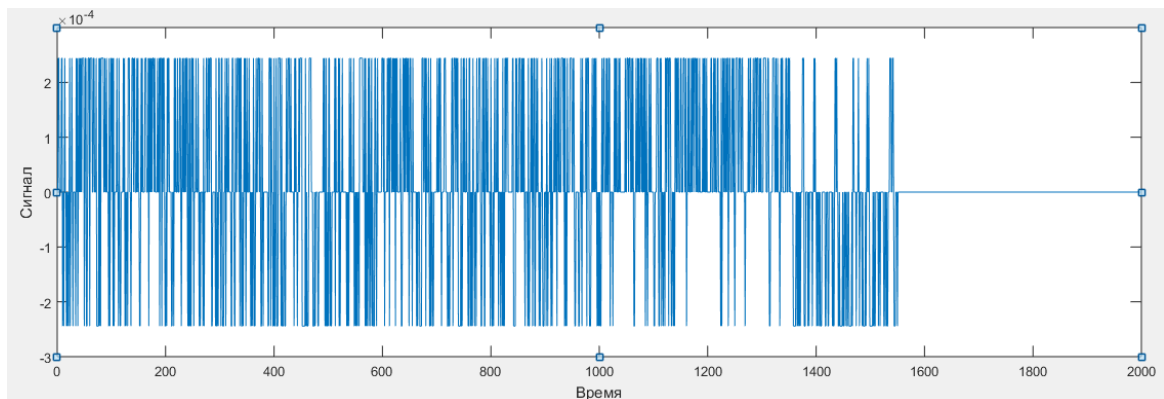


Рис. 5в. Разность амплитуд заполненного (4 бита) и пустого контейнера

Отметим более значительное искажение контейнера при использовании 4 бит для кодирования.

На рис. 6а-6в представлены наложение амплитуды пустого аудиоконтейнера большого размера (длительностью более 5 минут) и заполненного аудиоконтейнера (500 символов).

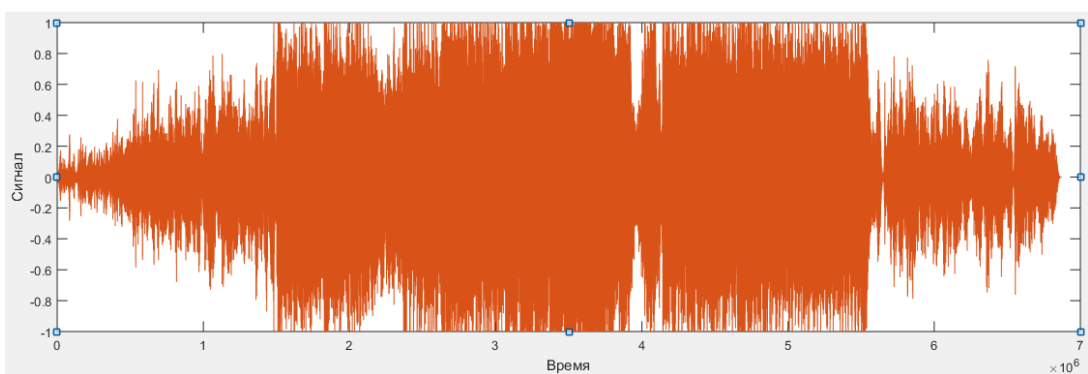


Рис. 6а. Пустой контейнер

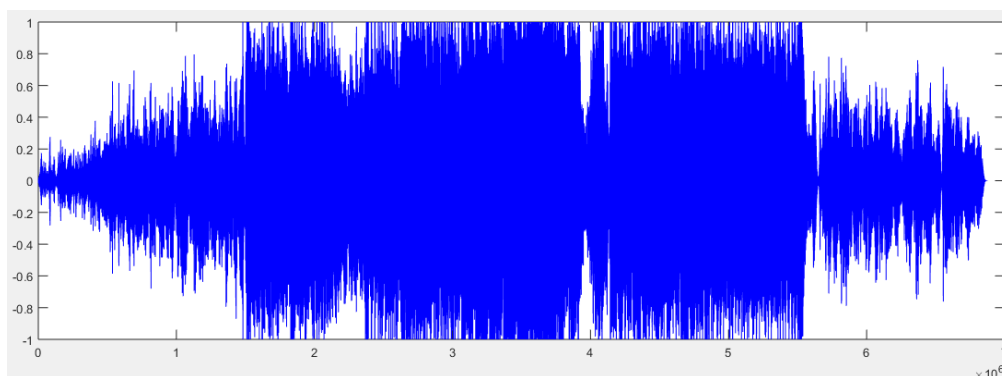


Рис. 6б. Заполненный контейнер (4 бита)

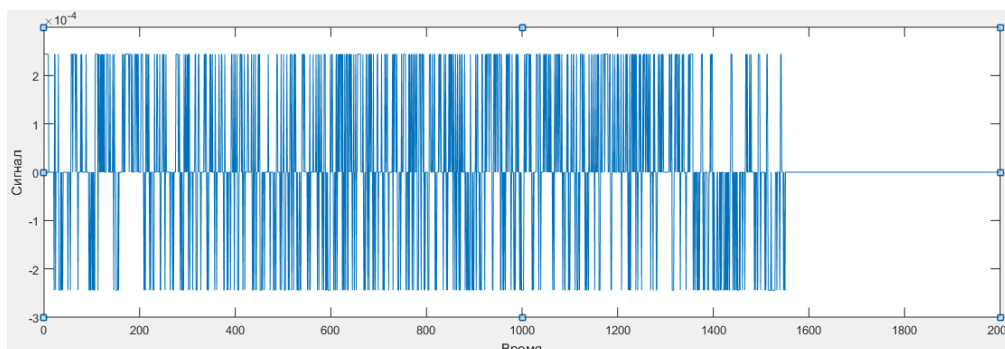


Рис. 6в. Разность амплитуд заполненного (4 бита) и пустого контейнера

Следует подчеркнуть, что при использовании контейнеров длительностью 96 и 311 сек, сокрытое сообщение (500 символов) занимает лишь небольшую часть контейнеров, таким образом, данные контейнеры могут быть использованы для сокрытия куда больших объемов информации.

Проведены эксперименты по оценке возможности устойчивого сокрытия графических данных [5]. Пример электрической принципиальной схемы приведен на рис. 7.

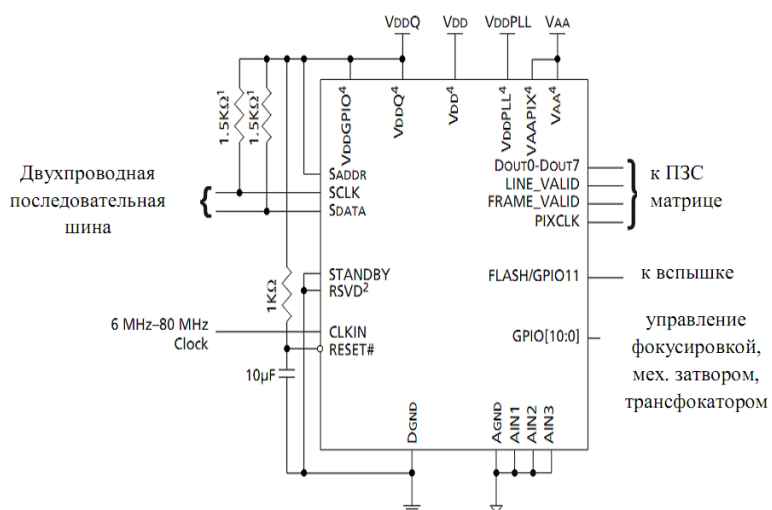


Рис. 7. Схема микроконтроллера ТВ - камеры

Экспериментально было установлено допустимое соотношение объемов аудиоконтейнера и скрываемой текстовой информации - 4.8% (Обзор источников показал, что допустимым соотношением для метода LSB принято считать 8%).

При проведении исследований ни на графиках, ни на слух искажений контейнера отмечено не было, однако оценка графиков разностей амплитуд позволяет предположить, что контейнеры с более сложной структурой позволяют скрывать информацию более эффективно.

В таблице 1 приведены численные результаты экспериментов – оценка искажений различных контейнеров в зависимости от количества кодируемых бит (в процентном соотношении). Размер сокрытого текстового сообщения в каждом контейнере – 500 символов.

Таблица 1

Оценка искажения исходных (пустых) контейнеров при кодировании различного числа бит

Длительность аудиоконтейнера (сек)	Количество кодируемых младших бит	
	2 бита	4 бита
3	0,6%	2,3%
96	0,0088%	0,039%
311	0,0086%	0,035%

Заключение

Разработано программное средство, позволяющее проводить выбор аудиоконтейнера для сокрытия проектной документации методом LSB. Полезность предложения подтверждена экспериментально: более сложная структура контейнера способствует более успешному сокрытию проектной документации.

Список литературы

- [1] Яценко В.В. Введение в криптографию. СПб.: Питер, 2001. 289 с.
- [2] Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. М.: МК-Пресс, 2006. 288 с.

- [3] Волосатова Т.М., Денисов А.В., Чичварин Н.В. Комбинированные методы защиты данных в САПР // Приложение к журналу «Информационные технологии». 2012. № 5. С. 1-32
- [4] Чичварин Н.В., Волосатова Т.М. Метод сокрытия данных в стереофонических аудиофайлах // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. 2015. № 9. Режим доступа: <http://engbul.bmstu.ru/doc/792392.html> (дата обращения 25.01.16).
- [5] Ремизов А.В., Филиппов М.В. Оценка необнаружимости стеганографических алгоритмов // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. 2012. № 3. DOI: 77.30569/359383.
- [6] Васина Т. С. Обзор современных алгоритмов стеганографии // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. 2012. № 4. DOI: 77- 30569/370605.