При использовании методов кодирования с расширением спектра ЦВЗ внедряется в аудиосигналы (последовательность 8- или 16-битных отсчетов) путем незначительного изменения амплитуды каждого отсчета. Сжатие MPEG и скользящие фильтры средних частот сильно искажают ЦВЗ, встроенный в аудиосигнал с помощью данного метода.

В методах маскирования ЦВЗ используется эффект, при котором более слабый звуковой сигнал становится неслышимым на фоне более сильного звукового сигнала (сигнала маскирования). Метод устойчив к применению ЦАП и АЦП, аддитивным шумам, которые «придерживаются» порога маскирования сигнала с ЦВЗ, фильтрации и сжатию. Для встраивания ЦВЗ с помощью данного метода требуется тщательный анализ контейнера.

Методы встраивания информации с использованием эхо-сигнала позволяют встраивать информацию, изменяя параметры эхо-сигнала [3]. Метод достаточно устойчив ко всем видам сжатия файла-контейнера, а также цифро-аналоговому и аналого-цифровому преобразованию, поскольку в данном случае скрываемая информация встраивается не в те участки, которые изменяются при преобразованиях файла-контейнера.

Для решения поставленной задачи наилучшими характеристиками обладает последний из описанных методов. В частности, алгоритм скрытия информации с помощью изменения времени задержки эхо-сигнала может разместить цифровую сигнатуру избыточно в потоке аудиоданных. В результате значительное количество спрятанной информации остается даже после таких операций, как извлечение или редактирование. Эта информация может быть, но это не всегда так, информацией об авторских правах. Также возможно применение метода с целью голосовой идентификации и голосовой аутентификации в телефонных линиях.

СПИСОК ЛИТЕРАТУРЫ:

1. *Иваненко В. Г., Кириллов И. А.* Защита авторского права на аудиоданные с помощью цифровых водяных знаков // Безопасность информационных технологий. 2008. № 3. С. 96–99.
2. *Грибунин В. Г., Оков И. Н., Туринцев И. В.* Цифровая стеганография. Салон-Пресс, 2002. – 272 с.
3. *Gruhl B., Lu A., Bender W.* Echo Hiding, Information Hiding Workshop. Cambridge, UK, 1996.

В. Г. Иваненко, Р. В. Солдатенко

ЗАЩИТА ПЕЧАТНОЙ ПРОДУКЦИИ С ПОМОЩЬЮ ТЕКСТУРНЫХ ВОДЯНЫХ ЗНАКОВ

Бумажные носители информации, несмотря на рост количества безбумажных процедур, остаются важным средством обмена информацией, взаиморасчетов и идентификации личности. Вопрос защиты печатной продукции стоит весьма остро, особенно при защите недорогой полиграфической продукции, такой как газеты, журналы, книги, буклеты. Специфика защиты подобной продукции заключается в стоимости — она должна, как минимум, не превышать стоимости самой продукции, поэтому полиграфические средства защиты в большинстве случаев не пригодны по экономическим соображениям.

Перспективной технологией защиты авторских прав является использование цифровых водяных знаков (ЦВЗ), под которыми понимаются специальные метки, незаметно внедряемые в цифровые данные для того, чтобы в дальнейшем существовала возможность их извлечения и

представления доказательств авторства этих данных [1]. Как правило, они основываются на цифровой модификации носителя информации — контейнера, однако в таком случае возникает проблема: модификацию контейнера нельзя представить на носителе информации — листе бумаги. Решить ее можно с помощью технологии текстурных водяных знаков (ТВЗ), которая основывается на том же принципе, что и ЦВЗ, только в таком случае изменению подвергается само изображение. Трудность подобного подхода заключается в поиске рационального соотношения между степенью невидимости ТВЗ и возможностью их последующего выделения из изображения.

В данной работе рассматривается один из способов встраивания ТВЗ, основанный на незаметном параллельном сдвиге некоторых участков изображения на некоторую величину под определенным углом [2]. В качестве изображения-носителя может приниматься любое черно-белое изображение. Важным преимуществом соответствующего алгоритма является то, что для встраивания ТВЗ не требуется специальных средств печати и сканирования — достаточно простых принтера и сканера. Для получения информации о наличии ТВЗ и извлечения ТВЗ нужно отсканировать это изображение, преобразовать его разрешение до разрешения исходного контейнера, программно наложить на него изображение-решетку, зная величину и угол смещения.

Приведем обобщенные характеристики выбранного алгоритма. После вывода стеганограммы на устройство печати метки ТВЗ должны быть невидимыми для зрительной системы человека. Степень их неразличимости зависит от определенных значений параметров, при удачном сочетании которых метки ТВЗ остаются невидимыми.

В случае, когда противник знает метод встраивания ТВЗ, для выделения ТВЗ из отсканированного изображения ему необходимо знать параметры периодической решетки-ключа (период и угол поворота), кроме того, противнику нужно знать разрешающую способность изображения — стеганограммы. Таким образом, для извлечения ТВЗ потенциальному противнику нужно подобрать 3 параметра, что представляется затруднительным для реализации в реальных условиях. Это позволяет считать выбранную систему достаточно безопасной.

Готовая стеганограмма устойчива к сжатию или компрессии (до определенных пределов), расширению, выделению (вырезанию) части изображения, изменению формата изображения. Эти относит выбранную стегосистему к системам с высокой робастностью.

Теоретически, максимальное количество информации, которое может быть встроено в 1 пиксель изображения контейнера, составляет 1 бит. В действительности, максимальное количество встраиваемой в контейнер информации Q оказывается ниже отмеченной величины. Его можно определить как $Q = k \cdot N_1 \cdot N_2$, где $N_1 (N_2)$ — разрешающая способность изображения — контейнера по горизонтали (вертикали), $k < \frac{1}{2}$. Кроме того, при $k = 1$ стеганограмма будет неотличима от контейнера даже после выделения в ней ЦВЗ.

СПИСОК ЛИТЕРАТУРЫ:

1. *Гончаренко М. В., Иваненко В. Г., Кириллов И. А.* Проблема защиты авторских прав на аудио и видеоданные с помощью цифровых водяных знаков // Безопасность информационных технологий. 2009. № 1. С. 99–100.

2. *Митекин В. А., Сергеев А. В., Федосеев В. А., Богомолов Д. М.* Модели стеганографической системы и обобщенного алгоритма встраивания ЦВЗ в полиграфические изделия // Компьютерная оптика. 2007. Том 31. № 4.