тем более развернутым будет вектор, описывающий поведение ПО, и тем более точными будут результаты моделирования и анализа.

В рамках данной работы разработаны три типа модели поведения: общая, точная и нейронная. Продемонстрированы преимущества и недостатки, а также показана область применения каждой модели. Представлены результаты выявления НДВ различного уровня сложности, заложенных в тестовый набор прикладного ПО с открытым кодом.

СПИСОК ЛИТЕРАТУРЫ:

1. *Марков А. С., Миронов С. В., Цирлов В. Л.* Выявление уязвимостей в программном коде // Открытые системы. М., 2005. № 12.
2. Круглый стол «Вестника Связи» // Вестник Связи. 2006. № 12. С. 4–18.

В. Г. Иваненко, С. В. Родченко

ВСТРАИВАНИЕ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ В АУДИОСИГНАЛЫ

В связи с бурным распространением сети Интернет весьма важной становится проблема защиты авторских прав на аудиоданные. Любой человек может разместить любые аудиофайлы в Сети, предварительно заявив, что он имеет права на них и является законным владельцем данной аудиопродукции. Для защиты соответствующих авторских прав возможно использование цифровой стеганографии, в частности технологии цифровых водяных знаков [1].

Цифровой водяной знак (ЦВЗ) — это специальная метка, незаметно внедряемая в изображение или другой сигнал с целью контроля его распространения. При этом ЦВЗ, содержащий информацию о законном владельце и правообладателе, встраивается в защищаемый аудиофайл для осуществления возможности проверки авторства, закрепленного за ним. Сама встроенная информация изменяет параметры аудиофайла незначительно (эти изменения «невидимы» для слушателя, что является важнейшей особенностью алгоритма встраивания), и при этом данная информация встраивается таким образом, чтобы злоумышленнику было трудно ее извлечь или разрушить, значительно не повредив при этом сам контейнер. Целевое же извлечение встроенной информации не представляет серьезных сложностей, поскольку другой стороне известны параметры встраивания.

Существует пять основных методов встраивания информации в аудиосигналы: методы кодирования наименее значащих бит, методы фазового кодирования, методы расширения спектра, методы маскирования цифровых водяных знаков, методы встраивания информации с использованием эхо-сигнала [2].

Методы кодирования наименее значащих бит по сравнению с другими перечисленными методами имеют худшие показатели стойкости для встраиваемых ЦВЗ.

В методах фазового кодирования, в зависимости от внедряемых данных, происходят модификация фазы начального сегмента аудиосигнала и согласование с ним фазы последующих сегментов для сохранения разности фаз. ЦВЗ, встроенный посредством данного метода, лишь частично переживает двойное цифро-аналоговое и аналого-цифровое преобразование. Возникают проблемы извлечения после перестановки сэмплов в аудиосигнале. Метод имеет достаточно хороший показатель невидимости встроенного ЦВЗ.

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