УДК 681.3.06:519.248.681

*Е. Г. КАЧКО, канд. техн. наук, С. С. БАТЮШКО*

# ИССЛЕДОВАНИЕ ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ «ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ» ДЛЯ ЗАЩИТЫ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

С развитием всемирной компьютерной сети Интернет и всеобщей доступностью вычислительных ресурсов все больше и больше информации, в том числе защищенной авторскими правами, хранится, воспроизводится и распространяется в электронном виде. Несмотря на такие преимущества как возможность неограниченного тиражирования, простой и быстрой доставки потребителю, данный метод имеет один, но весьма существенный недостаток – неэффективность традиционных средств защиты интеллектуальной собственности как технических, так и правовых.

По этой причине электронное пиратство и присвоение авторских прав приобрело просто угрожающие размеры. Особенно большие потери, связанные с подобного вида нарушениями, несут аудио- и видеозаписывающие студии, т. е. организации, занимающиеся распространением графической, аудио- и видеопродукции, записанной в цифровом формате. Несанкционированное тиражирование с последующей продажей нелицензионных аудио- и видеокомпакт-дисков стало во многих странах одним из наиболее прибыльных видов бизнеса, приносящего многомиллиардные доходы пиратам в сфере электронных технологий. Большое распространение такой незаконной деятельности характерно для стран, в которых цивилизованные законы рынка еще не занимают господствующего положения.

Сегодня на первый план выходит проблема разработки программных систем, способных обеспечивать надежную защиту авторских прав. Одним из перспективных путей решения этой проблемы может послужить использование «цифровых водяных знаков» (Digital watermarking), которые позволяют автоматически обнаруживать авторство произведенного программного продукта и достаточно эффективно осуществлять защиту авторских прав.

С помощью «цифровых водяных знаков» осуществляется встраивание специфического электронного знака в исходное изображение или аудиозапись для идентификации владельца авторских прав на данную информацию. Вместе с данными об авторе в качестве знака могут быть встроены также данные о конкретном экземпляре, такие как серийный номер, имя владельца и т. п.

В целом сама технология «цифровых водяных знаков» делится на две большие области. Первая – это собственно «цифровые водяные знаки», которые используются для скрытия информации об авторских правах. Вторая – это встраивание в производимый аудио-, видеопродукт «цифровых отпечатков пальцев», которые используются для скрытия серийных номеров или иной информации, позволяющей отличить копии носителя одну от другой.

В основу принципа действия «цифровых водяных знаков» положен тот факт, что в поток исходных данных, записанных в цифровом формате (изображение или звук), можно внести некоторые искажения (изменения), несущие дополнительную информацию, практически неразличимые человеческими органами зрения или слуха и в силу этого не снижающие потребительские качества исходного сигнала.

Несмотря на то, что технология «цифровых водяных знаков» имеет сравнительно короткую историю, на сегодняшний день можно утверждать, что уже теоретически разработаны и проходят соответствующую апробацию десятки, если не сотни, алгоритмов создания соответствующих компьютерных программ данного типа [1 – 2]. Их анализ позволяет рассмотреть некоторые принципы и свойства, которые являются общими для всех. Рассмотрим эти свойства.

- Невидимость: добавление электронного «водяного знака» не должно ухудшить исходный сигнал. Такой знак не должен быть заметен человеческим глазом. Это свойство «водяных знаков» конфликтует со следующими двумя.
- Устойчивость: «водяной знак» должен сопротивляться манипуляциям, которые могут возникнуть при использовании продукта, таких как фильтрация, сканирование и печать, преобразование в другие форматы.
- Защита: «водяной знак» должен сопротивляться попыткам его удаления. Это не абсолютное требование, скорее оно привязано к уровню ухудшения несущего сигнала. Грубая атака, разрушающая исходный сигнал, также может разрушить и «водяной знак».
- Публичность: используемый алгоритм «водяных знаков» должен являться открытым. Как и в криптографии, «защищенность через скрытность» не является верной концепцией. Сохранение метода «водяных знаков» в секрете приводит к тому, что он лишается постороннего анализа, тем самым становясь потенциально менее защищенным.
- Многократность водяных знаков: должна существовать возможность внесения в исходный сигнал нескольких водяных знаков одновременно.
- Масштабируемость: должна существовать возможность использования более новых, улучшенных версий той же технологии при доступности более мощных вычислительных средств. Это означает, например, использование больших по длине криптографических ключей. И в то же время система должна быть устойчивой при более мощных вычислительных ресурсах.
- Самовосстановление: если только некоторый фрагмент несущего сигнала доступен, например, после усечения или поворота изображения, должна существовать возможность восстановления «водяного знака».
- Возможность использования совместно со сжатым битовым потоком: эта возможность особенно полезна для программ реального масштаба времени.
- Сопротивление «столкновению» (усреднению): если несколько изображений, помеченных различными «водяными знаками», усредняются, результат тоже должен быть помеченным. Эта возможность нужна в двух ситуациях: а) при подписи, где одно и то же изображение помечается по-разному для различных заказчиков и б) для пометки видео, где несколько похожих кадров могут быть усреднены.

Следует отметить, что для использования электронных «водяных цифровых знаков» в видеопродукции существуют также и общие дополнительные требования. Среди них наиболее важными являются:

- Возможность добавления «водяных знаков» в реальном режиме.
- Не увеличивать поток передаваемых данных (полосу пропускания).

Поскольку электронный «цифровой водяной знак» должен быть невидимым, устойчивым к различным типичным операциям над изображениями, таким как применение алгоритмов сжатия, фильтрациии изображения (сглаживание краев, изменение контраста и т. п.) и геометрических трансформаций (масштабирование и т. п.), то «цифровой водяной знак» должен храниться не в формате файла, а непосредственно в самом изображении.

Еще одной из областей применения «цифровых водяных знаков» является проверка целостности изображений, то есть выяснение того, что в исходное изображение не внесены какие-либо изменения. Это стало особенно актуально сейчас, когда уровень программного обеспечения достиг такого рубежа, что уже практически невозможно отличить оригинал от подделки.

Использование «цифровых водяных знаков» находит применение и в стеганографии (от греческого – тайнопись). С помощью стеганографических методов появляется возможность невидимого встраивания некоторого количества данных в исходный сигнал. Это дает возможность обмениваться шифрованными сообщениями без привлечения внимания третьей стороны [3]. Как правило, в применяемых в стеганографии алгоритмах большее внимание уделяется объему скрываемых данных и их незаметности, чем устойчивости к повреждениям. В этом своем качестве стеганография весьма близка к криптографии. Вместе с тем, между стеганографией и криптографией имеются как сходства, так и существенные различия.

Общеизвестно, что одной из областей применения криптографии является шифрование данных для передачи через коммуникационные каналы с целью скрытия их содержимого. Сам факт передачи зашифрованного сообщения не скрывается. Стеганография же предполагает имплантацию секретного сообщения в какую-либо форму несущих сигналов, обычно в изображение или видеопоток, объективно определяемую как наличие шума или помех. Без правильного ключа практически невозможно не только извлечь скрытое сообщение, но даже определить его присутствие. Стеганографические сообщения, как правило, шифруются для увеличения безопасности, надежности в передаче данных. При этом возможно комплексное сочетание принципов криптографии и стеганографии. В этом случае информация вначале надежно шифруется, а затем еще и дополнительно прячется. В имеющихся на эту тему единичных открытых публикациях отмечается, что для того, чтобы спрятать подобные секретные сообщения в графических файлах, в большинстве случаев используются торальные автоморфизмы [4 – 5] или потоки Колмогорова [6].

Важным сходством между криптографией и «цифровыми водяными знаками» является использование симметричных и несимметричных шифровальных систем.

Технология встраивания «водяных знаков» может быть основана на использовании так называемых пространств преобразования. В этом случае к исходному изображению применяют некоторые обратимые операции перед встраиванием самого знака. После этого изображение встраивается (изменяются некоторые коэффициенты преобразования), и эти действия проделываются вновь для получения «меченого» изображения. Трансформации, которые обычно используются для этого, могут быть следующими: дискретное косинусное преобразование, дискретное преобразование Фурье, фрактальное преобразование, дискретное wavelet-преобразование. Реже применяются преобразования Френеля, комплексное wavelet-преобразование, преобразование Фурье-Меллина.

Использование различных пространств преобразования дает определенные преимущества: поскольку «водяной знак», встроенный в пространстве преобразования, распределен в изображении иррационально, то его, следовательно, сложно выделить или изменить. Более того, частотное изменение изображения позволяет выбрать только определенные (наилучшие) участки исходного изображения для внесения «водяных знаков».

Рассматриваемая технология встраивания электронных «цифровых водяных знаков», как представляется, является весьма эффективной и том смысле, что не только надежно прячет информацию, но и защищает ее от несанкционированного взлома и деформаций.

Во-первых, обеспечивается необходимая в таких случаях противозашумленность конфиденциальной информации. Это свойство вытекает из того факта, что атакующий не знает привилегированной информации, которой обладают отправитель и получатель. Как результат, атакующий должен зашумить весь спектр широкополосного сигнала. Но зашумление имеет ограниченную возможность, поэтому атакующий может зашумить каждую частоту с малой силой, в то время как отправитель и получатель имеют значительное преимущество по соотношению сигнал-шум. В применении к встраиванию «водяных знаков» это означает, что для того, чтобы разрушить «водяной знак», нужно в изображение внести такие помехи, что оно становится непригодным для дальнейшего использования.

Во-вторых, это весьма малая вероятность перехвата. Это свойство основано на том, что большой сигнал распределяется по всему частотному спектру, поэтому только ничтожно малые изменения добавляются к каждой частоте. Часто такое приращение меньше уровня помех, поэтому атакующий не сможет даже определить наличие сигнала. Это позволяет «водяным знакам» быть более защищенными [7].

Одним из перспективных направлений развития стеганографических технологий является использование в процессе встраивания «цифровых водяных знаков» так называемых псевдошумов. В этом случае в качестве несущего берется такой сигнал, для которого статистические свойства как можно более близки к свойствам истинно случайного сигнала, объективно воспринимаемого как шум. При этом истинный сигнал может быть в точности воспроизведен, если известны некоторые привилегированные (секретные) параметры. К примеру, в качестве несущей может быть использован выход генератора случайных чисел, который был инициализирован с помощью некоторого начального числа, известного только владельцу. В этом смысле использование псевдошумов оказывается очень полезным, поскольку дополнительно затрудняет для атакующего выделение «цифрового водяного знака», а следовательно, и конфиденциальной информации из исходного изображения.

Использование стеганографических методов предполагает глубокое знание свойств человеческих органов зрения и слуха и, прежде всего, порога их чувствительности к изменениям изображения или звука. Если говорить коротко, то «цифровые водяные знаки» в этом смысле должны обеспечивать:

- контрастную маскировку – т.е. невозможность обнаружения человеческими органами зрения одного сигнала в присутствии другого сигнала;
- частотную маскировку – т.е нечувствительность человеческого глаза к изменившимся волновым решеткам на разных частотах;
- световую маскировку – т.е. не преодолевать порога чувствительности к световым изменениям на контрастном фоне;
- непреодоление порога ощущения различий – т.е порога, за которым любые изменения соответствующего коэффициента кажутся практически неразличимыми [8].

Таковы лишь некоторые особенности использования стеганографических методов, которые могут быть применены для защиты интеллектуальной собственности, а также найти свое применение при передаче конфиденциальной информации в электронном виде. Стремление ведущих компаний, работающих в сфере аудио- и видеобизнеса, обезопасить себя от электронного пиратства делает весьма актуальным разработки программных продуктов, решающих эту важную задачу.

**Список литературы**: 1. *Walter Bender, Daniel Gruhl, Norishige Morimoto, and A. Lu.* Techniques for data hiding. IBM Systems Journal, 1996. 35 (3-4). Pp. 313 – 336. 2. *Ingemar J. Cox and Matt L. Miller.* A review of watermarking and the importance of perceptual modeling. In Bernice E. Rogowitz and Thrasyvoulos N. Pappas, editors, SPIE Human Vision and Electronic Imaging II. February 1997. Vol. 3016, Pp. 92 – 99. 3. *Zenon Hrytskiv, Sviatoslav Voloshynovskiy, and Y. B. Rytsar.* Cryptography and steganography of video information in modern communications. In Proceedings of the 3rd International Conference on Telecommunications in Modern Satelite, Cable and Broadcasting Services TELSIKS '97, Vol. 1, Pp 164 – 167. 4. *George Voyatzis and Ioannis Pitas.* Application of toral automorphisms in image watermarking. In Proceedings of the IEEE International Conference on Image Processing, ICIP '96. Vol. 2, Pp. 237 – 240. 5. *George Voyatzis and Ioannis Pitas.* Digital image watermarking using mixing systems. Computer & Graphics, August. 1998. 22(4). Pp. 405 – 416 6. *Josef Scharinger.* Robust watermark generation for multimedia copyright protection. In Markus Vincze, editor, Robust Vision for Industrial Applications. 1999. Pp. 127 – 136. 7. *Зюко А.Г., Кловский Д.Д., Назаров М.В., Финк Л.М.* Теория передачи сигналов. М.: Радио и связь, 1988. 8. *Raymond B. Wolfgang, Christine I. Podilchuk, and Edward J. Delp.* Perceptual watermarks. for digital images and video. Proceedings of the IEEE, Special Issue on Identication and Protection of Multimedia Information, July 1999. 87(7). Pp. 1108 – 1126.

*Харьковский национальный*

*университет радиоэлектроники*

*Поступила в редколлегию 29.04.2003*