Секция 4

МАТЕМАТИЧЕСКИЕ МЕТОДЫ СТЕГАНОГРАФИИ

УДК 519.6

МЕТОД ЗАЩИТЫ ОТ НЕЛЕГАЛЬНОГО КОПИРОВАНИЯ
В ЦИФРОВЫХ ВИДЕОТРАНСЛЯЦИЯХ ЧЕРЕЗ ВНЕДРЕНИЕ
ВОДЯНЫХ ЗНАКОВ ПРИ РАСШИФРОВАНИИ

В. А. Анжин

Предложен метод защиты передаваемого в рамках цифровой видеотрансляции материала от копирования, в котором цифровые водяные знаки, идентифицирующие клиента, внедряются в видеоматериал на этапе его расшифровки клиентом. В основе метода лежит использование поточного шифра, позволяющего для заданного ключа зашифрования и набора позиций компонент защищаемого материала строить такой ключ расшифрования, при расшифровании на котором значения на предварительно указанных позициях инвертируются относительно их значений в исходном открытом тексте, а на всех остальных компонентах остаются совпадающими с соответствующими значениями в исходном открытом тексте.

Ключевые слова: защита от копирования, видеотрансляция, цифровые водяные знаки.

В наши дни абсолютное большинство информации хранится, передаётся и обрабатывается в цифровой форме. Это даёт возможность унифицировать часть этапов работы с данными, но вместе с тем порождает вопросы защиты авторских прав. Наиболее остро проблемы защиты от неограниченного нелегального копирования встали перед производителями произведений искусства, распространяемых в цифровой форме. В их числе, среди прочих, находятся и поставщики цифрового видео.

Поставщик видеоматериала может устанавливать получателям правила доступа к распространяемым данным. Они могут быть разными, но первичным является запрет на самостоятельное перераспространение полученного материала легальными клиентами. Кроме того, необходимо ограничение возможности доступа сторонних лиц к каналам связи между сервером распространения и клиентами. Для этого применяют шифрование распространяемых данных.

Основным подходом к решению проблемы нелегального копирования является юридическое ограничение такой возможности и добавление в каждую распространяемую копию скрытого идентификатора, позволяющего однозначно определить источник утечки. Такой скрытый идентификатор называют цифровым водяным знаком. Внедрение водяных знаков может осуществляться на различных этапах видеокодирования [1], в том числе и в закодированное видео.

При распространении цифрового видео возможно использование различных подходов к внедрению водяных знаков:

- использование доверенного декодера [2], работающего на стороне клиента. Водяной знак внедряется после декодирования цифрового видео до его передачи пользователю;

- предварительная подготовка множества копий с внедрёнными водяными знаками;
- внедрение водяного знака на этапе передачи.

Другим подходом, исследуемым в данной работе, является использование крипто-системы, позволяющей для данного ключа зашифрования и набора некоторых компонент цифрового видео, индивидуальных для каждого клиента, строить такой ключ расшифрования, при расшифровании на котором значения этих компонент инвертируются относительно их значений в исходном открытом тексте, а значения всех остальных его компонент сохраняются совпадающими с их значениями в исходном открытом тексте. Номера инвертируемых компонент выбираются такими, что изменение значений этих компонент не приводит к заметному искажению видеоматериала.

Для каждого из клиентов подготавливается уникальный ключ расшифрования, известный только производителю видеоматериала. Передаваемая мультимедиа информация единожды шифруется и доставляется конкретному потребителю вместе с программой расшифрования по «зашитому» в ней ключу расшифрования, сгенерированному для этого клиента. Клиент осуществляет расшифрование полученного шифртекста, в процессе которого в материал автоматически вносятся изменения, идентифицирующие получателя.

Требуемое шифрование и расшифрование можно выполнить, например, на базе поточного шифра с фильтрующим генератором ключевого потока.

Ключом в нём является тройка $(F_1(x), F_2(x), iv)$, где $F_1(x)$ — фильтрующая функция; $F_2(x)$ — используемый в регистре с линейной обратной связью (LFSR) полином; iv — начальное заполнение (состояние) регистра.

Процедура построения ключа расшифрования $(F'_1(x), F'_2(x), iv')$ для данного ключа зашифрования $(F_1(x), F_2(x), iv)$ и позиции k , при расшифровании на котором получится изменённый в k -й позиции открытый текст, может выглядеть следующим образом:

- 1) Отсчитываем k первых тактов работы LFSR, изначально заполненного iv , с полиномом обратной связи $F_2(x)$.
- 2) Фиксируем в LFSR текущее состояние $a = a_1 a_2 \dots a_n$ и образуем моном $x^a = x^{a_1} x^{a_2} \dots x^{a_n}$. Здесь n — длина регистра.
- 3) $F'_2(x) = F_2(x)$, $iv' = iv$, $F'_1(x) = F_1(x) + x^a$.

Для обоснования работоспособности метода осуществлена его практическая реализация для формата видеокодирования MPEG-2 Video. Для внедрения водяных знаков в закодированное в этом формате видео использован метод «Low Complexity Watermarks for MPEG Compressed Video» из [3].

ЛИТЕРАТУРА

1. *Mistry D.* Comparison of digital water marking methods // Int. J. Comp. Sci. Engin. 2010. V. 2. No. 9. P. 2905–2909.
2. *Wang P.* Tamper Resistance for Software Protection. A Thesis for the Degree of Master of Science. Information and Communications University, Daejeon, Korea, 2005.
3. *Langelaar G. C.* Real-time Watermarking Techniques for Compressed Video Data. Delft: Delft University of Technology, 2000. 155 p.