



Программно-аппаратные методы защиты информации

Лекция 14

Цифровые водяные знаки

Цифровыми водяными знаками (ЦВЗ, Digital Watermarking) называется практически невоспринимаемое изменение объекта с целью погружения дополнительного сообщения об этом ПС. Обычно дополнительное сообщение представляет собой идентификационный код собственника ПС. Иногда факт погружения должен оставаться неизвестным для посторонних. ЦВЗ должны быть устойчивы к естественным преобразованиям. Главное отличие стеганографии и ЦВЗ. В стеганографии факт погружения не должен обнаруживаться, а защита от преднамеренного удаления не всегда необходима. ЦВЗ не обязательно должны быть необнаруживаемы, но, как правило, защищены от удалений и ложных погружений.

Объектами для ЦВЗ могут служить различные медиафайлы:

- неподвижные изображения,
- подвижные изображения (видео и TV),
- аудио ПС (речь и музыка),
- графические представления текстов и схем,
- коды источников (для программ),
- топология микро чипов,
- описание химических формул,
- интернет-протоколы.

Модели ЦВЗ и их классификация:

- с известным объектом для легального декодера (информированный кодер),
- с неизвестным объектом для легального декодера («слепой» декодер),
с использованием объектом в легальном кодере (информированный кодер),
- конфиденциальные ЦВЗ (только авторизованные пользователи могут извлекать ЦВЗ),
- общедоступные ЦВЗ (любой пользователь может извлечь ЦВЗ),
- «0»-бит ЦВЗ (погруженное сообщение состоит лишь в факте его погружения определенным пользователем),
- многобитовые ЦВЗ (погруженное сообщение состоит из нескольких бит).

Основные применения систем с ЦВЗ:

- Мониторинг рекламы.
- Идентификация собственника ПС.
- Доказательство прав собственности на ПС.
- Отслеживание сделок (Fingerprinting).
- Аутентификация содержания ПС.
- Управление копированием.
- Управление устройствами считывания.

Мониторинг рекламы.

Рекламодатель хочет быть уверенным, что под его рекламу по электронным средствам (радио, TV, интернет), действительно, задействованы определенные объемы каналов вещания.

Пассивный мониторинг рекламы предполагает участие человека-оператора или автоматизацию в ограниченных объемах.

Активный мониторинг основан на погружении специальной информации в рекламный продукт, которая затем может автоматически извлекаться.

Для цифровых объектов, активный мониторинг возможен при помощи использования идентификационных кодов в специальных коротких заголовках рекламных продуктов. Использование ЦВЗ позволяет наиболее тесно связать рекламный продукт и идентификационный код рекламодателя.

Идентификация собственника

Эта функция ЦВЗ служит для уточнения данных о собственнике объекта. Когда декодер обнаруживает ЦВЗ, он связывается с центральной базой данных по интернету и использует ЦВЗ, как ключ для получения контактной информации о собственнике объекта.

Доказательство прав собственности.

Разница с предыдущим случаем – ЦВЗ нужны для доказательства прав собственности в суде.

Собственник, благодаря использованию ЦВЗ, может избежать регистрационных расходов для своих произведений.

Отслеживание сделок

В этом случае ЦВЗ содержит сведения о легальных покупателях (“fingerprinting”), что позволяет отследить, кто из них оказался в дальнейшем нелегальным распространителем копий.

Аутентификация содержания объекта.

В криптографии широко известны методы аутентификации (например, цифровая подпись (ЦП)).

Присоединение ЦП к аутентифицируемым сообщениям создает риск ее потери при передаче по сети или преднамеренного удаления.

ЦВЗ дают возможность погружать ЦП непосредственно в объект без заметного искажения последних.

Управление копированием

Эта функция ЦВЗ не преследует цели отслеживания нелегальных распространителей копий (пиратов). Она обеспечивает невозможность (или нецелесообразность) нелегального копирования.

Управление устройствами.

Обобщением функции «управление копированием» является функция «управление устройствами», когда устройство может реагировать на обнаруженный в ПС ЦВЗ.