УДК 003.26

ЦИФРОВЫЕ ВОДЯНЫЕ ЗНАКИ КАК МЕТОД ЗАЩИТЫ ИЗОБРАЖЕНИЯ

А.А. СИВОГРАКОВ
(Представлено: канд. физ.-мат. наук., доц. Ю.Ф. ПАСТУХОВ)

В данной статье представлена классификация нанесения цифровых водяных знаков. Разобраны виды алгоритмов встраивания по направлениям, выделены их основные преимущества и недостатки.

Введение. В эпоху компьютеров, наиболее распространенными нарушениями интеллектуальной собственности являются: плагиат, «пиратство», изменение информации, подделка информации, недобросовестная конкуренция.

При хранении, распространении и передачи интеллектуальной собственности, зачастую в качестве защиты, используют цифровые водяные знаки. Цифровой водяной знак (ЦВЗ) – это специальная метка, встраиваемая в цифровой сегмент, с целью тем или иным образом отслеживать распространение информации по сетям связи, обеспечивать поиск информации в мультимедийных базах данных. Цифровой водяной знак, применительно к изображению как правило не видим, то есть изначальное изображение, и изображение со встроенным ЦВЗ, визуально неотличимы зрительной системой человека.

Классификация ЦВЗ. Впервые термин «Digital watermarking» был введен в работе [1]. Он получил свое название от способа защиты от подделки ценных бумаг. В настоящее время разработаны различные методы нанесения ЦВЗ, классификация которых представлена на рисунке 1.

Рисунок 1. – Классификация методов ЦВЗ

Встраиваемый знак может быть как видимый глазу, так и не видимый. Второй вариант более распространен и делится на хрупкие, стойкие (робастные) и полухрупкие ЦВЗ. В случае хрупкой системы ЦВЗ, водяной знак разрушается после любых незначительных изменений контейнера. Такие знаки необходимы для аутентификации сигнала (цифровые отпечатки пальцев). Робастные знаки наоборот должны переносить многие виды атак: аффинные преобразования (повороты, обрезание), сжатие и другие. Как раз такие знаки и используются для определения авторства, так как их сложно разрушить. Полухрупкий ЦВЗ – это знак с избирательной сложностью. Такой знак может допускать определенные преобразования контейнера, разрушаясь от других [3].

Алгоритмы встраивания делятся на обратимые и необратимые. Обратимые алгоритмы позволяют извлечь водяной знак и полностью восстановить контейнер для дальнейшей работы. Такие алгоритмы применяются для медицинских и военных целей, где любые искажения изображений категорически запрещены. Необратимые алгоритмы при извлечении ЦВЗ вносят изменения в первоначальный контейнер, поэтому при разработке таких алгоритмов цель разработчика заключается в снижении уровня искажений до минимума.

В более сложных обратимых методах можно выделить алгоритмы, основанные на модификациях гистограмм изображения и алгоритмы, основанные на преднамеренной регулировке значения разности между соседними парами пикселей. Первая группа является простой в реализации и использует минимум информации для декодера, недостатками же является ограничение объема встраивания, который зависит

от количества вхождений точек максимума яркости. Вторая группа алгоритмов позволяет встраивать в сообщение большие объемы информации, но при этом ухудшается качество маркированного изображения.

Различают линейные и, соответственно, нелинейные методы нанесения ЦВЗ, а также методы использующие фрактальное кодирование, основанное на предположении, что изображение самоподобно [2]. Линейные алгоритмы делятся на алгоритмы встраивания (аддитивные), когда цифровое изображение добавляется в цифровое сообщение, и алгоритмы слияния (fusion), когда в одно изображение встраивается другое, например, логотип.

Так же множеством разработчиков было предложено использование корреляционных алгоритмов. Но использование таких алгоритмов оправдано, если пользователю необходимо извлечь скрытое сообщение, и основной контейнер воспринимается как шум (необратимый метод). Главным преимуществом алгоритмов слияния перед алгоритмами встраивания является допущение легкое искажение ЦВЗ при извлечении.

Алгоритмы пространственной области внедряют ЦВЗ в исходное изображение. Их преимуществом является то, что нет необходимости выполнять преобразования изображений. ЦВЗ в таких методах обычно внедряется засчет манипуляций яркостью или цветовыми составляющими. Недостатком таких алгоритмов является довольно слабая устойчивость к различным операциям обработки изображений.

Частотные алгоритмы, основанные на преобразованиях изображения, реализуются сложнее, т.к. перед внедрением ЦВЗ необходимо «перераспределить энергию» контейнера, чтобы встроить сообщение в специальные спектральные области. За счет подобной декомпозиции изображения ЦВЗ становится робастным к атакам.

Наибольшую сложность представляет внедрение ЦВЗ в низкочастотную область, содержащую большую часть энергии изображения, потому что неоптимальное внедрение может привести к значительному искажению контейнера. Данная сложность является одновременно и преимуществом, поскольку любая попытка злоумышленника извлечь ЦВЗ из низкочастотной области также приведет к значительному искажению изображения. Таким образом, при встраивании ЦВЗ в частотную область изображения необходимо соблюдение компромисса между объемом встраиваемого ЦВЗ и качеством стеганоконтейнера [4].

Методы, основанные на моментах изображений, применяются для защиты ЦВЗ от геометрических преобразований контейнера. Однако они имеют узкую направленность, а их основным недостатком является низкий уровень безопасности от других видов атак.

Заключение. Цифровые водяные знаки на данный момент являются наиболее эффективным средством защиты авторских прав на произведения мультимедиа. Это один из основных способов предотвращения нарушений авторских врав в интернете. Это сфера быстро развивается, поэтому существует множество разных видов и типов встраивания. На сегодняшний день существует большое количество методов внедрения ЦВЗ, каждый из которых обладает своими достоинствами и недостатками, которые надо учитывать при использовании того или иного метода для защиты мультимедийных данных от незаконного распространения и модификации.

ЛИТЕРАТУРА

1. Osborne C., vsn Schyndel R., Tirkel A. A Digital Watermark // IEEE Intern. Conf. on Image Processing, 1994. P. 86-90.
2. Грибунин В.Г., Оков И.Н., Туринцев В.И. Цифровая стеганография. – М. : СОЛОН-Пресс 2002. 272 с.
3. Балакин А.В., Елисеев А.С., Гуфан А.Ю. / Использование стеганографических методов для защиты текстовой информации. – М. : Т-comm Телекоммуникации и транспорт, 2009. С 42–50.
4. Elshoura, S.M. A secure high capacity full-gray-scale-level multi-image information hiding and secret image authentication scheme via Tchebichef moments / S.M. Elshoura, D.B. Megherbi // Signal Processing: Image Communication. 2013. – Vol. 28. P. 531–552.