УДК 004.932

А. В. Афанасьева, Д. О. Иванов, Д. А. Рыжов

АЛГОРИТМ ВСТАВКИ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ ПРИ ИСПОЛЬЗОВАНИИ СТАНДАРТА H.264

Предложен алгоритм вставки цифровых водяных знаков (ЦВЗ) в видеопоток, закодированный по стандарту H.264. Описан способ согласования алгоритма извлечения ЦВЗ с антикоалиционными кодами.

Ключевые слова: *H.264, цифровые водяные знаки, антикоалиционные коды.*

Введение. Фильмы, а также другая видеопродукция часто подвергаются нелицензионному распространению, при этом правообладатели не получают прибыли. Для борьбы с таким неконтролируемым распространением видеопродукции можно использовать метод внесения индивидуального цифрового водяного знака (ЦВЗ) в каждую продаваемую копию фильма. Этот знак будет содержать идентификационную информацию о покупателе копии. Тогда по каждой нелицензионно распространяемой копии можно будет установить ее покупателя. Чтобы недобросовестные покупатели не уничтожали ЦВЗ, он должен быть устойчив к различным видам атак. Особое внимание необходимо обратить на коалиционные атаки, при которых несколько недобросовестных покупателей, используя свои копии, создают новую.

Задача защиты видеопродукции при помощи ЦВЗ может быть разделена на четыре этапа: построение множества идентификационных меток, внедрение одной из меток в видеопоследовательность, извлечение метки из пиратской копии видеопоследовательности, поиск участников коалиции по извлеченной метке.

Как правило, для работы с видеопотоком (вставка и извлечение метки) применяются алгоритмы обработки видеоданных, использующие специфические модели потока и атакующего, а при построении пространства меток и обнаружении участников пиратской коалиции применяются алгоритмы, разработанные в рамках теории помехоустойчмвого кодирования. Цель настоящей статьи — построить схему согласованной работы алгоритмов этих двух типов. Рассмотрим разработанные независимо решения для двух задач и на их базе предложим новый интегрированный подход. В работе исследуются методы вставки ЦВЗ для видеопотоков, сжатых в формате H.264, так как этот формат наиболее популярен и используется в различных приложениях.

Алгоритмы вставки ЦВЗ. При вставке цифровых водяных знаков в сжатый видеопоток возможно использовать только декодирование энтропийного кода, так как процедура полного перекодирования потока отнимает много вычислительных ресурсов, что создает дополнительные трудности при распространении видеопродукции. После декодирования энтропийного кода можно извлечь из потока (и следовательно, внести информацию) векторы движения и квантованные частотные коэффициенты дискретного косинусного преобразования (ДКП) макроблоков. Метод изменения частотных коэффициентов обеспечивает устойчивость к атакам при фиксированном уровне вносимых искажений, поэтому его активно исследуют [1—5], и в настоящей статье он тоже использован.

DC	$AC_{0,1}$		
$AC_{1,0}$	$AC_{1,1}$		

Рассмотрим блок 4×4 (см. рисунок) после применения ДКП и квантования, он состоит из основного DC коэффициента и набора AC коэффициентов, упорядоченных по частоте. Выделенные на рисунке низкочастотные AC коэффициенты содержат большую часть энергии, поэтому изменять нужно именно их, это обеспечит стойкость к атакам, связанным с обработкой кадра. Алго-

ритм вставки характеризуется тремя параметрами: глубина продавливания коэффициентов (L), количество изменяемых коэффициентов в блоке и число изменяемых блоков в кадре, он основан на правиле:

$$AC_{i,j} = AC_{i,j} \pm L,$$

знак определяется передаваемым битом. Стоит отметить, что для детектирования необходим исходный блок. Задав эти параметры, можно получить информационную емкость одного кадра.

Для определения сочетаний предельно допустимых значений параметров, не приводящих к существенному ухудшению визуального качества, алгоритма был исследован ряд видеофрагментов. Для оценки вносимых искажений применялся ряд метрик (SSIM, PSNR), а также проводилось субъективное визуальное оценивание. Для того чтобы вносимые искажения нельзя было заметить, необходимо на этапе предвычислений для вставки выбирать текстурные блоки (содержащие мало ненулевых коэффициентов). Отметим, что метод выбора блоков „открыт“, а секретным ключом является изменяемый коэффициент. Задачей атакующего будет угадывание коэффициента для изменения, так как если он изменит все коэффициенты, то произойдет значительная потеря в качестве.

Антикоалиционные коды. Существует несколько классов антикоалиционных кодов, стойкость которых к атакам с заданным размером коалиции доказана [6, 7]. Эти коды отличаются от кодов, исправляющих ошибки, тем, что вместо алгоритма декодирования используют алгоритм поиска участников коалиции по искаженной метке. Оба класса позволяют выявить участников коалиции, если она не превышает заданного размера, при этом гарантируется, что с высокой степенью вероятности будет найден хотя бы один участник. Основными параметрами таких кодов являются:

— число пользователей в системе,

— предполагаемый максимальный размер коалиции,

— параметр безопасности системы.

Поскольку коды Тардоша [7] имеют минимальную длину последовательностей благодаря своей вероятностной природе, то для исследований были выбраны именно они. Использование более коротких кодов позволит сократить долю используемых блоков, доступных для вставки, уменьшить количество вносимых искажений и повысить уровень обеспечиваемой безопасности.

Коды Тардоша предназначены для борьбы с коалиционными атаками и мало исследованы на стойкость к шумовым атакам (случайным искажениям не обнаруженных участниками коалиции битов). В настоящей статье была смоделирована атака шумом на коды Тардоша, благодаря чему удалось выяснить, что при даже небольшом проценте шума (2—3 %) вероятность обвинения невиновного пользователя высока. В работе [7] рассмотрена возможность проведения шумовых атак и предложен способ борьбы с ними путем удлинения кодов, Однако антикоалиционные коды имеют очень большую длину (до 2 МБ), поэтому такой путь решения нежелателен.

Для того чтобы данные коды можно было использовать без удлинения, нужно снизить влияние шума на вероятность ошибки при определении злоумышленника. Для решения этой задачи модель канала, используемая в алгоритме поиска, должна быть лучше согласована с реальным каналом, т.е. необходимо использовать дополнительную информацию, получаемую при извлечении битов метки из видеопоследовательности. В частности, использование при принятии решения об извлекаемом бите не только знака отклонения частотного коэффициента, но и амплитуды позволит определить уровень надежности полученных символов. Для лучшего соответствия модели каналу был введен новый символ — стирание. Он помещается в извлеченную последовательность, когда невозможно точно определить, какой символ передавался — 0 или 1. При поиске участников коалиции по извлеченному кодовому слову стертые позиции не учитываются, т.е. код укорачивается.

Было смоделировано воздействие различных уровней шума и стираний на извлеченную последовательность. Результаты показывают, что с ростом уровня шума вероятность ошибочного определения злоумышленника увеличивается, а с ростом уровня стираний — почти сохраняется. Эксперименты показали также, что данная замена не уменьшает вероятность определения злоумышленника. Таким образом, если, к примеру, из 30 % шума на последовательность 10 % шума удастся заменить стираниями, то вероятность ошибки уменьшается более чем на 25 %.

С помощью предложенного метода вставки и извлечения ЦВЗ в тестовый набор видео последовательностей были внедрены метки, после чего был проведен ряд атак. Результаты экспериментов показали, что наиболее успешны атаки постфильтрации и уменьшения размера кадра, которые приводят к 19—21 % ошибок извлечения. При использовании на этапе извлечения дополнительных символов стирания вероятность ошибки извлечения снижается с 19—21 до 0,6 %.

Заключение. Коды Тардоша позволяют успешно бороться с коалиционными атаками пользователей, однако требуется их значительное удлинение для обеспечения стойкости к шумовым атакам. Шумовые атаки неизбежны, так как предложенный метод вставки ЦВЗ позволяет не избежать ошибок, а только снизить их вероятность до 20 %. При этом использование символов стираний в кодах Тардоша дает снижение вероятности ошибки обнаружения злоумышленника при исходной длине кода.

СПИСОК ЛИТЕРАТУРЫ

1. *Su P.-C., Li M.-L., Chen I.-F.* A content-adaptive digital watermarking scheme in H.264/AVC Compressed videos // Proc. Intern. Conf. on Intelligent Information Hiding and Multimedia Signal Processing. 2008. P. 849—852.

2. *Su P.-C., Chen I.-F., Chen C.-C.* A practical design of digital video watermarking for content authentication // Signal Processing: Image Communication. 2011. P. 413—426.

3. *Saryazdi S., Demehri M.* A blind dct domain digital watermarking // Sciences of Electronic, Technologies of Information and Telecommunicatios. 2005. P. 55—57.

4. *Mansouri A., Aznaveh A. M., Torkamani-Azar F., Kurugollu F.* A low complexity video watermarking in H.264 compressed domain // IEEE Transact. on Information Forensics and Security. 2010. Vol. 5, N 4. P. 649—657.

5. *Беззатеев С. В., Литвинов М. Ю., Трояновский Б. К., Филатов Г. П.* Выбор алгоритма преобразования, обеспечивающего изменение структуры изображения // ИУС. 2006. № 6(25). С. 2—6.

6. *Boneh D., Shaw J.* Collusion-Secure Fingerprinting for Digital Data // IEEE Transact. on Information Theory. 1998. Vol. 44, N 5. P. 1897—1905.

7. *Tardos G.* Optimal probabilistic fingerprint codes // Proc. ACM Symp. on Theory of Computing. NY, USA, 2003. P. 116—125.

Сведения об авторах

Александра Валентиновна Афанасьева — магистр; Санкт-Петербургский государственный университет аэрокосмического приборостроения, кафедра безопасности информационных систем; программист; E-mail: alra@vu.spb.ru

Денис Олегович Иванов — Санкт-Петербургский государственный университет аэрокосмического приборостроения, кафедра безопасности информационных систем; программист; E-mail: denis.ivo@vu.spb.ru

Дмитрий Алексеевич Рыжов — аспирант; Санкт-Петербургский государственный университет аэрокосмического приборостроения, кафедра безопасности информационных систем; E-mail: dr@vu.spb.ru

Рекомендована кафедрой
№ 51 безопасности информационных систем

Поступила в редакцию
01.02.13 г.