

ЗАЩИТА ВИДЕОПОСЛЕДОВАТЕЛЬНОСТИ В АЛГОРИТМАХ КОДИРОВАНИЯ MPEG

Н.А. Лавринович

Кафедра электронных вычислительных средств,
Белорусский государственный университет информатики и радиоэлектроники
Минск, Республика Беларусь
E-mail: nlavri@gmail.com

Предложен метод защиты видеопоследовательности на основе скремблирования видеопотока с использованием случайной числовой последовательности большого периода. Определены возможности интеграции механизмов защиты в новые стандарты кодирования семейства MPEG.

ВВЕДЕНИЕ

С ростом объемов разного рода информации, растет необходимость контроля ее потребления. Проведение исследований по защите видеоинформации в контексте стандартов кодирования видео семейства MPEG наиболее актуально. Лидером индустрии по праву можно считать стандарт H.264. Его дальнейшее развитие и внедрение продолжено в стандарте H.265.

Подход к защите видеоданных по схемам с открытым или закрытым ключом, использующих блочные алгоритмы, такие как AES, DES, ГОСТ после алгоритмов кодирования, требуют больших вычислительных затрат, что приводит к ограничению возможности использования классического шифрования, так как система должна обеспечивать хорошую производительность в реальном времени, без задержек расшифровывать, а затем декодировать и отображать полученное видео.

Другие подходы защиты видео последовательности базируются на интеграции алгоритма в структуру стандарта кодирования видео, как, например, это показано в [1], где изменяется последовательность считывания квантованных коэффициентов дискретного косинусного преобразования (ДКП), и выполняется шифрование коэффициентов по алгоритму DES.

Существует метод выборочного шифрования, в котором шифруются только низкочастотные составляющие ДКП [2]. Другой предложенный способ [3], предусматривает в каждом сегменте кадра перестановку значений коэффициентов ДКП, занимающих одну и ту же позицию в матрице, с использованием некоторой таблицы правил перестановки. Внутри каждого сегмента осуществляется изменение случайным образом знаков коэффициентов ДКП, перестановка векторов движения P-кадров, а также знаков этих векторов.

Аналогичный метод предлагает выборочное шифрование только битов, отвечающих за знак коэффициентов ДКП в I-, P- и B-кадрах, что существенно снижает требования к вычислительным ресурсам.

Также интересен метод шифрования частей данных поступающих на этап энтропийного кодирования [4] для стандартов H.265 и H.264. При соблюдении ряда правил и ограничений, такой метод позволяет сохранить исходный битрейт видеопотока, структуру совместимую с декодером, при этом, достаточно эффективно зашифровать нужную информацию с помощью алгоритма шифрования AES в режиме обратной связи по шифротексту. В данном случае, шифруются только значащие части векторов движения, в некоторых случаях, разностных коэффициентов и, для стандарта H.265, некоторых блоков отвечающих за структуризацию бинарной информации для энтропийного кодера. Особенностью является то, что процесс прозрачно совмещен с энтропийным кодированием и дает неплохие результаты при субъективном наблюдении искаженного изображения.

1. МЕТОД ЗАЩИТЫ ВИДЕОПОСЛЕДОВАТЕЛЬНОСТИ

В отличие от описанных выше подходов предлагается шифровать поток видеоданных стандарта H.264 с помощью скремблирования квантованных результатов ДКП [5]. Сгенерированная случайная последовательность большого периода, полученная с помощью генератора псевдослучайных чисел (ГПСЧ) «вихрь Мерсенна» подвергается хешированию для улучшения криптографических свойств. Далее происходит наложение полученной последовательности на квантованные коэффициенты ДКП. С целью снижения вычислительных затрат, шифрование векторов движения в данном случае не происходит.

Рассмотрены различные варианты скремблирования исходного изображения (см. рис. 1): выборочное и полное скремблирование коэффициентов, изменение только DC коэффициентов закодированного макроблока (DC коэффициенты трансформированные преобразованием Адамара в режиме кодирования INTRA16x16), изменение только AC коэффициентов закодированного макроблока, различные комбинации таких режимов. Лучшие результаты были получены в трех случаях: скремблирование всех DC коэф-

фициентов (см. рис. 2), скремблирование нулевых DC коэффициентов и ненулевых AC коэффициентов (см. рис. 3), скремблирование всех DC коэффициентов и ненулевых AC коэффициентов (см. рис. 4).



Рис. 1 – Исходное изображение.



Рис. 2 – Скремблирование всех DC коэффициентов.



Рис. 3 – Скремблирование нулевых DC и ненулевых AC коэффициентов.



Рис. 4 – Скремблирование всех DC и ненулевых AC коэффициентов.

Таблица 1 – Временные затраты и объем зашифрованного файла

Режим скремблирования	Время, с	Объем, Мб	Сжатие, раз
Без скремблирования	46,375	1,6	27
DC коэффициенты.	46,965	3,8	11
Нулевые DC коэффициенты. и ненулевые AC коэффициенты.	47,121	5,5	8
DC коэффициенты и ненулевых AC коэффициенты.	47,426	6,1	7

Как видно из таблицы 1, первый вариант дает наименьшее снижение степени сжатия и

наименее требователен к вычислительным ресурсам, позволяя достичь хорошего уровня искажения исходного изображения.

II. ДАЛЬНЕЙШИЕ ИССЛЕДОВАНИЯ

Новые возможности стандарта H.265 предлагают древовидную структуру представления кадра [6], которая имеет свое отражение в синтаксисе результирующего потока данных, что совместно с алгоритмами перестановки, может использоваться для искажения реальной картины разбиения кадра.

Возросшее количество вариантов внутрикадрового предсказания блока [6] (тридцать пять вариантов против восьми в стандарте H.264), дает более широкие возможности по подмене индекса используемого предсказания, например, скремблированием или табличной подстановкой. Такой механизм искажения информации не влияет на сами данные кодирования (результаты преобразований, предсказаний движения) и минимально влияет на качество последующего энтропийного сжатия. Восстановления картинки с неверным предсказанием может серьезно ухудшить субъективное восприятие, за исключением больших областей одного цвета.

ЗАКЛЮЧЕНИЕ

Методы защиты видеоинформации снижают степень сжатия в два и более раз. Однако, предложенный метод требует меньше вычислительные ресурсы по сравнению с классическим шифрованием закодированного видеопотока. Актуальным видится поиск алгоритма защиты, незначительно влияющего на степень компрессии, например, на основе энтропийного сжатия или подмены индексов предсказаний.

1. Tang L. Methods for encrypting and decrypting MPEG video data efficiently / L. Tang // In Proceedings of the ACM Multimedia, November 18-22, 1996, Boston, USA. – P. 219–229.
2. Yongcheng L. Security Enhanced MPEG player / L. Yongcheng, C. Zhigang, T. See-Mong, R. H. Campbell // IEEE First International Workshop on Multimedia Software Development, March 25-26, 1996, Berlin, Germany. – P. 169–175.
3. Wenjun Z. Efficient Frequency Domain Selective Scrambling of Digital Video / Z. Wenjun, L. Shawmin // IEEE Transactions on Multimedia. – 2003. – P. 118–129.
4. Loïc Dubois. Selective encryption of images and videos: from JPEG to H.265/HEVC through JPEG2000 and H.264/AVC / Loïc Dubois, Zafar Shahid, William Puech // Progress in Data Encryption Research / Camel Tanougast. – New York: Nova Publishers, – 2013. – P. 137–178.
5. Лавринович Н. А. Кодирование видео со скремблированием / Н.А. Лавринович // Доклады БГУИР. – 2013. – №5. – С. 55–60.
6. Gary J. Sullivan, Jens-Rainer Ohm, Woo-Jin Han, Thomas Wiegand. Overview of the High Efficiency Video Coding (HEVC) Standard. IEEE transactions on circuits and systems for video technology, Vol. 22, No. 12, December 2012. – 2003. – P. 1649–1668.