УДК 004.056.2

Электронная подпись видеопотока

В. Г. Насенник

Предлагается очень простая схема электронной подписи видеопотока, позволяющая выделять из видеопотока любой непрерывный фрагмент, для которого сохраняются свойства электронной подписи не только в отношении установления авторства и отсутствия модификации каждого отдельного кадра, но и отсутствия монтажа, т.е. изменения последовательности кадров.

Ключевые слова: ЭЦП, электронная подпись, видеопоток.

1. Введение

Применение электронной подписи видеопотока имеет особую актуальность в связи с использованием видеозаписей в качестве документов. Наряду с широким распространением средств записи видео также развиваются программные и технические средства редактирования видеозаписей и даже их фальсифицирования (”deepfake”). Отличие видео от других видов информации заключается в том, что длина видеопотока в общем случае неизвестна. По этой причине традиционные технологии электронной подписи имеют весьма ограниченное применение – только для подписывания уже готовых видеофайлов конечной длины. Электронная подпись каждого отдельного кадра также не имеет особого смысла, поскольку сохраняется возможность видеомонтажа – изготовления видеоряда из видеокадров с изменением порядка их следования с целью искажения смысла происходивших событий, зафиксированных на видео.

В литературе известны попытки решения этой задачи [1], не получившие, однако, широкого практического распространения. В настоящей статье предлагается чрезвычайно простой протокол электронной подписи видеопотока, гарантирующий не только отсутствие модификаций любого конкретного кадра, но и неизменность последовательности кадров, в том числе в любом произвольном фрагменте, выделенном из видеопотока.

2. Определения

Определим видеопоток как последовательность кадров:

$$..., F_i, F_{i+1}, F_{i+2}, F_{i+3}, ...$$

Число кадров в общем случае неограничено. Если применяется какая-либо технология сжатия видео, то каждый кадр представляется уже в сжатом виде, в котором он будет в дальнейшем храниться и передаваться. Алгоритмы сжатия видео не рассматриваются в данной статье [2].

Определим как H_i результат вычисления криптографической хэш-функции:

$$H_i = hash(F_i).$$

Определим D как результат вычисления электронной подписи S для данных T с использованием ключа подписи SK:

$$D = S_{SK}(T).$$

Определим функцию проверки электронной подписи с использованием ключа проверки электронной подписи PK, связанного с ключом подписи SK:

$$C_{PK}(T, D).$$

Эта функция возвращает логическое значение ВЕРНО, если электронная подпись D соответствует данным T при использовании ключа PK, и логическое значение НЕВЕРНО во всех остальных случаях.

Алгоритмы вычисления хэш-функции, вычисления электронной подписи, проверки электронной подписи, а также все остальные аспекты, связанные с применением электронной подписи и криптографии с открытым ключом, в данной статье не рассматриваются [3].

Термины электронная подпись, цифровая подпись, электронная цифровая подпись и ЭЦП являются синонимами. [4]

3. Постановка задачи

Требуется разработать технологию электронной подписи видеопотока неопределённой длины с тем условием, чтобы можно было выделить любой непрерывный фрагмент этого видеопотока и использовать его с сохранением всех свойств электронной подписи – установления авторства, невозможности отказа от авторства, удостоверения целостности каждого отдельного кадра в этом фрагменте, а также непрерывности и порядка следования кадров.

4. Решение задачи

Решение этой задачи оказалось удивительно простым. Для этого достаточно при вычислении электронной подписи использовать конкатенацию значений хэш-функций от текущего кадра и предыдущего

$$D_i = S_{SK}(H_{i-1} \parallel H_i),$$

где оператор $\parallel$ означает конкатенацию.

Электронная подпись вычисляется непосредственно в устройстве, осуществляющем съёмку видео и сжатие видеопотока. Вычисленная электронная подпись вместе со значениями хэш-функций присовокупляется к соответствующим кадрам.

$$..., (F_i, H_{i-1}, H_i, D_i), (F_{i+1}, H_i, H_{i+1}, D_{i+1}), ...$$

При проверке электронной подписи видеопотока или фрагмента выполняются следующие проверки:

1. Проверить, что значение H_i равняется $hash(F_i)$ для текущего кадра.

2. Используя функцию $C_{PK}(H_{i-1} \parallel H_i, D_i)$, удостовериться, что электронная подпись D_i соответствует текущему кадру.

3. Проверить, что значение H_{i-1} равняется $hash(F_{i-1})$. Эта проверка производится для всех кадров за исключением самого первого.

Успешное выполнение всех этих проверок гарантирует, что каждый из кадров не изменялся, а также сохраняется последовательность кадров.

5. Заключение

Очевидно, эта технология может быть расширена. Вместе с видеокадрами при вычислении электронной подписи может быть включена дополнительная информация – оцифрованный

звук, сведения о месте и времени совершения видеозаписи по информации от приёмника спутниковой навигации (ГНСС) и т.д. В таком виде эта технология может найти применение при видеонаблюдении за выборами, при видеодокументировании следственных и процессуальных действий, в автомобильных видеорегистраторах и т.д.

Литература

1. *Gennaro R., Rohatgi P.* How to Sign Digital Streams. Information and Computation 1997, №165(1). P.100 – 116.
2. ITU-T Recommendation H.264|ISO/IEC International Standard ISO/IEC14496-10. Advanced video coding for generic audiovisual services. 2003. URL:http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=11466.
3. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке С. Триумф, 2012. 815 с.
4. ГОСТ 34.10-2018. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.

Статья поступила в редакцию 01.10.2021.

Насенник Виталий Геннадьевич
e-mail: vitaly.nasennik@gmail.com, ORCID: 0000-0002-7654-6953.

Separable Digitally Signed Video

V. Nasennik

A very simple scheme of a video stream electronic signature is proposed allowing us to isolate any continuous fragment from the video stream in respect of which the property of an electronic signature is preserved not only with respect to establishing authorship and the absence of modification of each individual frame but also the absence of editing i.e. changing the sequence of frames.

Keywords: computer security, public key cryptography, digital signatures, video.