DOI: 10.55648/1998-6920-2023-17-1-46-51 УДК 004.056.2

Анализ схемы электронной подписи видеопотока

Е. П. Мачикина

Сибирский гос. унив. телекоммуникаций и информатики (СибГУТИ)

Аннотация: В статье анализируется схема электронной подписи видеопотока, предложенная в статье В. Г. Насенника (2021 г.) и обладающая свойством сепарабельности, т.е. возможностью выделять произвольный фрагмент видеопотока, в отношении которого сохраняются все свойства электронной подписи. Предложенная технология имеет достаточно простую реализацию и относится к немасштабируемым «хрупким» методам, при этом информация для аутентификации не встраивается в изображение, а передаётся в метаданных. В статье проводится анализ возможных уязвимостей схемы и предлагаются возможные пути их устранения. Предлагаемые модификации схемы электронной подписи видеопотока позволяют исключить редактирование последовательности кадров или подменить видеопоток, при этом порядок трудоемкости модифицированной схемы остается прежним.

Ключевые слова: электронная подпись, видеопоток, методы аутенфикации видеопотока.

Для цитирования: Мачикина Е. П. Анализ схемы электронной подписи видеопотока // Вестник СибГУТИ. 2023. Т. 17, № 1. С. 46–51.
https://doi.org/10.55648/1998-6920-2023-17-1-46-51.

Статья поступила в редакцию 10.10.2022;
переработанный вариант – 20.12.2022;
принята к публикации 12.01.2023.

1. Введение

Широкое распространение видеоинформации во многих сферах человеческой деятельности требует надежных методов аутентификации видеоинформации. Под аутентификацией видеоинформации понимаются способы установления целостности видеоинформации, её подлинности и авторства.

Среди методов аутентификации видеоинформации можно выделить «хрупкие» криптографические методы, которые обнаруживают искажение даже единственного бита, и «робастные» методы, которые толерантны к небольшому количеству непреднамеренных искажений, возникающих, например, в канале передачи, но обнаруживают преднамеренные искажения видеоинформации.

По способу внедрения служебной информации методы аутенификации видеопотока делятся на явные, когда информация для аутентификации передаётся в служебных метаданных, и скрытые, когда информация для аутентификации внедряется непосредственно в изображение при помощи методов стеганографии (технология «цифровых водяных знаков»). Кроме того, существуют гибридные методы, сочетающие в себе явные и скрытые способы аутентификации видеопотока [1].

Также методы аутентификации мультимедийных потоков делятся на масштабируемые и немасштабируемые [2]. Немасштабируемые методы предназначены для ситуаций, когда защищаемый видеопоток передаётся в том же самом формате и разрешении, в каком записывался, и для аутентификации потока нужны все биты исходного потока. Масштабируемые методы предназначены для ситуаций, когда пользователи получают видеопоток с различными разрешениями в зависимости от своих потребностей и возможностей.

В статье [3] предложена технология сепарабельной электронной подписи видеопотока неопределённой длины, не имеющая обособленного начала или конца, позволяющая выделять произвольный фрагмент, в отношении которого сохраняются все свойства электронной подписи. Предложенная технология относится к немасштабируемым «хрупким» методам, при этом информация для аутентификации не встраивается в изображение, а передаётся в метаданных. К её достоинствам можно отнести простоту реализации.

В [3] видеопоток рассматривается как непрерывная последовательность кадров:

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

Для осуществления электронной подписи видеопотока неопределённой длины при вычислении подписи каждого кадра предлагается вычислять подпись от конкатенации хэш-функции текущего кадра и предыдущего:

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

где оператор $\parallel$ означает конкатенацию, а SK – ключ электронной подписи.

Вычисленная электронная подпись вместе со значениями хэш-функций присовокупляется к соответствующим кадрам:

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

Присовокупление уже вычисленных значений хэш-функций в поток выглядит избыточным, но имеет практическую пользу для ситуации, если вычисления хэш-функции и проверки электронной подписи могут быть распараллелены. Если не включать вычисленные значения хэш-функций в поток, то сначала придётся их вычислить, прежде чем приступить к проверке электронной подписи. Включение вычисленных значений хэш-функций в поток позволяет приступать к проверке электронной подписи параллельно с вычислением значения хэш-функции. Разумеется, принятие решения о том, что подпись соответствует, осуществляется только после того, как успешно проведено сравнение вычисленного значения хэш-функции и значения, указанного в потоке.

По сравнению с [4] в рассматриваемой схеме [3] нет особого первого блока, необходимого для проверки подписи всех последующих блоков, или особого последнего блока, необходимого для проверки подписей всех предыдущих блоков, что позволяет приступать к проверке электронной подписи видеопотока с произвольного места. Это позволяет, например, выделять произвольный фрагмент видеопотока, сохранить и использовать его отдельно, т.е. придаёт свойство сепарабельности этому методу аутентификации.

Однако в предложенной схеме [3] есть уязвимости, позволяющие осуществлять необнаруживаемое редактирование последовательности кадров или даже проводить атаки с подменой видеопотока. Далее будут приведены описания найденных уязвимостей и возможные пути их устранения.

2. Атака по статичным изображениям

В [3] неявно подразумевается, что разные кадры видеопотока будут между собой различны, однако это предположение не только не доказывается, но даже и не приводится.

Предположим, что осуществляется наблюдение за режимным помещением или урной для голосования со стационарной камеры. В этом случае значительную часть времени изображение будет статично. В обсуждаемой схеме электронной подписи видеопотока подпись осуществляется после операции сжатия. Несмотря на то, что в аналоговом видеосигнале всегда присутствует шум, при сжатии изображения с потерями этот шум отфильтровывается, и в результате возможно появление одинаковых кадров в видеопотоке. От одинаковых кадров значение хэш-функции также будет одинаковым: если $F_i = F_j, i < j$, тогда и $H_i = H_j$, где $H_i = \texttt{hash}(F_i)$. Если такие кадры найдены в видеопотоке, то весь фрагмент от i-го кадра до $j-1$ может быть удалён или повторён произвольное число раз.

Для борьбы с этим способом изменения подписанного видеопотока схему подписи необходимо модифицировать. Тут возможны, как минимум, два решения.

1) Нумерация кадров. Для этого каждому кадру должен быть присвоен свой уникальный достаточно длинный номер. Если использовать 32-битный номер, то при частоте 30 кадров в секунду и непрерывном круглосуточном видеонаблюдении этого хватит, чтобы обеспечить уникальную нумерацию в видеопотоке на протяжении приблизительно 4.5 лет. Вместо номера кадров лучше применить метку времени (timestamp), в которой явным образом закодированы дата и время съёмки каждого кадра:

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

При этом нужно модифицировать вычисление хэша и включить в вычисление номер кадра:

$$H_i = \texttt{hash}(i \parallel F_i).$$

Таким образом, даже при идентичных изображениях хэши от разных кадров с высокой вероятностью окажутся различными.

2) Сцепление хэшей. Для этого в вычисление хэша от текущего кадра нужно включить хэш от предыдущего кадра:

$$H_i = \texttt{hash}(H_{i-1} \parallel F_i).$$

Поскольку хэш от предыдущего кадра уже использован при вычислении хэша текущего кадра, то можно упростить вычисление подписи:

$$D_i = S_{SK}(H_i).$$

При таком сцеплении хэшей можно подписывать не каждый кадр, а реже – например, каждый n-й кадр или только опорные кадры в группе кадров. [2] Это снизит вычислительную нагрузку как на устройство, осуществляющее подпись, так и на устройство, проверяющее электронную подпись.

Эти два способа могут быть скомбинированы:

$$H_i = \texttt{hash}(H_{i-1} \parallel i \parallel F_i).$$

3. Подмена потока на запись от другой даты

Рассмотрим подмену видеопотока, снятого в одно время, на видеопоток, снятый в том же месте этой же камерой в другое время и подписанный этим же ключом электронной подписи. При подмене передача оригинального видеопотока каким-либо способом прерывается, а вместо него передаётся ранее записанный видеопоток.

Краткое прерывание транслируемого видеопотока может быть проигнорировано обслуживающим персоналом, поскольку поток будет содержать похожее изображение, подписанное надлежащим ключом электронной подписи.

Для борьбы с этой уязвимостью надо в качестве номера кадра или в дополнение к нему использовать метку времени TS (timestamp), включающую в себя в явном виде дату и время каждого кадра:

$$...(i, F_i, H_{i-1}, H_i, TS_i, D_i), ...,$$

где TS_i – метка времени.

При просмотре или проверке электронной подписи эта информация должна отображаться и обязательно контролироваться.

4. Подмена похожих видеопотоков

Во время видеонаблюдения нередки ситуации, когда различные видеопотоки имеют незначительные отличия. Например, производится наблюдение за похожими помещениями в режимном объекте или за похожими избирательными урнами. При этом аналоговые видеокамеры подключаются к многоканальному устройству, сжимающему изображение и осуществляющему электронную подпись этих видеопотоков с использованием одного и того же ключа электронной подписи. Из общих соображений информационной безопасности очевидно, что это неудачное решение, но в [3] оно не было запрещено явным образом, зато привлекательно для разработчиков аппаратуры по причине экономии ресурсов.

Чтобы избежать описанной уязвимости, небходимо включить в видеопоток уникальный идентификатор видеопотока, а при просмотре видеопотока или проверке электронной подписи этот идентификатор должен отображаться и контролироваться.

5. Заключение

С учётом упомянутых способов устранения уязвимостей усиленная схема электронной подписи видеопотока может выглядеть следующим образом:

$$H_i = \mathtt{hash}(H_{i-1} \parallel i \parallel ID \parallel TS_i \parallel F_i),$$

$$D_i = S_{SK}(H_i),$$

$$...(i, F_i, H_{i-1}, H_i, ID, TS_i, D_i), ...,$$

где i – номер кадра, F_i – кадр, H_i – хэш кадра, D_i – электронная подпись кадра, ID – уникальный идентификатор видеопотока, например, обозначение места съёмки, TS_i – метка времени (timestamp).

По сравнению с объёмом видеокадра затраты, связанные с добавлением в видеопоток этой дополнительной информации, пренебрежимо малы, зато предложенные решения устраняют выявленные уязвимости, а объём связанных с этим дополнительных вычислений также пренебрежимо мал.

Литература

1. *Мартимов Р. Ю.* Классификация методов защиты целостности видеоданных // Материалы III международной научной конференции «Технические науки: проблемы и перспективы», Санкт-Петербург, 2015. С. 44–46.
2. *Hefeeda M., Mokhtarian K.* Authentication schemes for multimedia streams: Quantitative analysis and comparison // ACM Transactions on Multimedia Computing, Communications and Applications. 2010. V. 6, Is. 1. P. 1–24.

3. *Насенник В. Г.* Электронная подпись видеопотока // Вестник СибГУТИ. 2021. № 4. С . 84–86.
4. *Gennaro R., Rohatgi P.* How to Sign Digital Streams // Information and Computation. 1997. № 165 (1). P. 100–116.

Мачикина Елена Павловна
к.ф.-м.н., доцент; доцент кафедры прикладной математики и кибернетики, Сибирский государственный университет телекоммуникаций и информатики (СибГУТИ, 630102, Новосибирск, ул. Кирова, д. 86), тел. +7 383 2698 272, e-mail: machikina@sibguti.ru, ORCID ID: 0009-0008-5512-4760.

Автор прочитала и одобрила окончательный вариант рукописи.
Автор заявляет об отсутствии конфликта интересов.

Analysis of Separable Digitally Signed Video

E. P. Machikina

Siberian State University of Telecommunications and Information Science (SibSUTIS)

Abstract: The article analyzes the electronic signature scheme for a video stream, proposed in the article by V. G. Nasennik (2021) and having the property of separability, i.e. the ability to select an arbitrary fragment of the video stream, in relation to which all the properties of the electronic signature are saved. The proposed technology has a fairly simple implementation and belongs to non-scalable ”fragile”methods, while authentication information is not embedded in the image, but is transmitted in metadata. The article analyzes the possible vulnerabilities of the scheme and suggests possible ways to eliminate them. The proposed modifications of the electronic signature scheme of the video stream make it possible to exclude editing of the sequence of frames or to replace the video stream, while the order of complexity of the modified scheme remains the same.

Keywords: electronic signature, video stream, video stream authentication methods.

For citation: Machikina E. P. Analysis of separable digitally signed video (in Russian). *Vestnik SibGUTI*, 2023, vol. 17, no. 1, pp. 46-51. https://doi.org/10.55648/1998-6920-2023-17-1-46-51.

The article was submitted: 10.10.2022;
revised version: 20.12.2022;
accepted for publication 12.01.2023.

References

1. Martimov R.Yu. Klassifikacija metodov zashhity celostnosti videodannyh [Classification of methods for protecting the integrity of video data]. *Materialy III mezhdunarodnoj nauchnoj konferencii «Tehnicheskie nauki: problemy i perspektivy»,* Sankt-Peterburg, 2015, pp. 44-46.
2. Hefeeda M., Mokhtarian K. Authentication schemes for multimedia streams: Quantitative analysis and comparison. *ACM Transactions on Multimedia Computing, Communications and Applications*, vol. 6, iss. 1, February 2010, pp. 1-24.

3. Nasennik V. G. Jelektronnaja podpis' videopotoka [Electronic signature of the video stream]. *Vestnik SibGUTI*, 2021, no. 4, pp. 84-86.
4. Gennaro R., Rohatgi P. How to Sign Digital Streams *Information and Computation*, 165(1), 1997, pp. 100-116.

Elena P. Machikina
Cand. of Sci. (Physics and Mathemathics), Docent; Docent of the Department of Applied Mathematics and Cybernetics, Siberian State University of Telecommunications and Information Science (SibSUTIS, Russia, 630102, Novosibirsk, Kirov St. 86), phone: +7 383 2698272, e-mail: machikina@sibguti.ru, ORCID ID: 0009-0008-5512-4760.