УДК 004.932.2

В.В. КОЛЕНКО, А.В. НАРОЖНЫЙ, канд. техн. наук, Херсон, Украина
В.М. ТОНКОНОГИЙ, д-р техн. наук, Одесса, Украина

ЗАЩИТА ДОСТОВЕРНОСТИ ЭЛЕКТРОННОГО ПОРТФОЛИО СТУДЕНТА НА ОСНОВЕ СТЕГАНОГРАФИЧЕСКИХ АЛГОРИТМОВ

Запропонований підхід до захисту достовірності інформації електронного портфоліо студента, який полягає в спільному використанні декількох інформаційно-технічних засобів захисту. У даній роботі запропоновано використовувати електронні цифрові підписи і цифрові водяні знаки.

Предложен подход к защите достоверности информации электронного портфолио студента, который заключается в совместном использовании нескольких информационно-технических мер защиты. В данной работе предложено использовать электронные цифровые подписи и цифровые водяные знаки.

Offered approach defence of authenticity of information of electronic portfolio student which consists in sharing of a few informative-technical measures of defence. In this work it is suggested to use electronic digital signatures and digital thread-marks.

«Традиционный» электронный портфолио студента (учащегося)представляет собой подборку, коллекцию работ, целью которой является демонстрация образовательных достижений учащегося и позволяет решить две основные задачи:

1. Проследить индивидуальный прогресс учащегося, достигнутый им в процессе получения образования, причем вне прямого сравнения с достижениями других учеников.

2. Оценить его образовательные достижения и дополнить (заменить) результаты тестирования и других традиционных форм контроля. В этом случае итоговый документ портфолио может рассматриваться как аналог аттестата, свидетельства о результатах тестирования (или выступать наряду с ними).

Основное требование для электронного портфолио — достоверность документов. В бумажном варианте сертификаты, грамоты, дипломы и пр. оформляются в соответствии с существующей традицией: скрепляются подписями ответственных лиц и печатью организации, выдавшей документ.

Аналогом является электронный документ, подписанный электронной цифровой подписью (ЭЦП).

Согласно украинского законодательства, электронная цифровая подпись — реквизит электронного документа, предназначенный для защиты электронного документа от подделки и позволяющий идентифицировать автора

документа, а также установить отсутствие искажения информации в электронном документе.

Электронная цифровая подпись обеспечивает защиту документа от искажения, подмены авторства, отказа от авторства. Однако для контроля доступа к информации, содержащейся в документе, этого недостаточно, требуются дополнительные методы. Цифровая подпись не привязана жестко к автору. Закрытым ключом для создания цифровой подписи может пользоваться любой человек, имеющий доступ к нему. Цифровую подпись можно сравнить с цифровой печатью, так как она обычно привязана к предприятию, отделу, учебному заведению, преподавателю, которые являются разделяемыми ресурсами. Конечно, доступ предоставляется только легитимным пользователям после соответствующей авторизации, а все действия протоколируются.

1. Цифровая подпись должна иметь свойства обычной подписи и одновременно должна являться цепью данных, которые можно передавать;
2. Цифровой подписью заверяются документы, которые передаются по сети. Цифровая подпись решает проблему возможных противоречий между отправителем и получателем;
3. Цифровая подпись должна быть уникальной, т.е. никто кроме автора не может создать такую же подпись, в том числе и особы, которые проверяют её аутентичность;
4. Каждый пользователь сети, законный или нет, в любой момент, в том числе и начальный, может проверить истинность цифровой подписи;
5. Тот, который подписал, не может отказаться от сообщения, документа и т.д. заверенного его цифровой подписью.

Чтобы удовлетворить всем перечисленным требованием цифровая подпись в отличие от «бумажной», должна зависеть от всех бит сообщений и изменяться даже при изменение одного бита подписанного сообщения.

Безопасность системы должна полностью определяться секретностью ключа. Это означает, что нарушитель может полностью знать все алгоритмы работы стегосистемы и статистические характеристики множеств сообщений и контейнеров, и это не даст ему никакой дополнительной информации о наличии или отсутствии сообщения в данном контейнере.

Заполненный контейнер должен быть визуально неотличим от незаполненного. Для удовлетворения этого требования надо, казалось бы, внедрять скрытое сообщение в визуально незначимые области сигнала. Однако, эти же области используют и алгоритмы сжатия. Поэтому, если изображение будет в дальнейшем подвергаться сжатию, то скрытое сообщение может разрушиться. Следовательно, биты должны встраиваться в визуально значимые области, а относительная незаметность может быть достигнута за счет использования специальных методов, например,

Сочетание ЭЦП и стеганографии повышает защищенность документа, однако, сами эти технические средства также требуют защиты. Ведь злоумышленник может изменить как цифровой знак, так и данные, контейнер или ЦВЗ.

К ЦВЗ предъявляются следующие требования:

- ЦВЗ должен легко (вычислительно) извлекаться законным пользователем.

- ЦВЗ должен быть устойчивым либо неустойчивым к преднамеренным и случайным воздействиям (в зависимости о приложения). Если ЦВЗ используется для подтверждения подлинности, то недопустимое изменение контейнера должно приводить к разрушению ЦВЗ (хрупкий ЦВЗ). Если же ЦВЗ содержит идентификационный код, ФИО преподавателя, логотип фирмы и т.п., то он должен сохраниться при максимальных искажениях контейнера, конечно, не приводящих к существенным искажениям исходного сигнала. Кроме того ЦВЗ должен быть робастным по отношению к аффинным преобразованиям изображения, то есть его поворотам, масштабированию. При этом надо различать устойчивость самого ЦВЗ и способность декодера верно его обнаружить. Скажем, при повороте изображения ЦВЗ не разрушится, а декодер может оказаться неспособным выделить его. Существуют приложения, когда ЦВЗ должен быть устойчивым по отношению к одним преобразованиям и неустойчивым по отношению к другим. Например, может быть разрешено копирование изображения (ксерокс, сканер), но наложен запрет на внесение в него каких-либо изменений.

- Должна иметься возможность добавления к стего дополнительных ЦВЗ. Лучшим выходом является добавление еще одного ЦВЗ, после которого первый не будет приниматься во внимание. Однако, наличие нескольких ЦВЗ на одном сообщении может облегчить атаку со стороны нарушителя, если не предпринять специальных мер.

Важной проблемой является определение подлинности полученной информации, то есть ее аутентификация. Обычно для аутентификации данных используются средства цифровой подписи. Однако, эти средства не совсем подходят для обеспечения аутентификации мультимедийной информации. Дело в том, что сообщение, снабженное электронной цифровой подписью, должно храниться и передаваться абсолютно точно, «бит в бит». Мультимедийная же информация может незначительно искажаться как при хранении (за счет сжатия), так и при передаче (влияние одиночных или пакетных ошибок в канале связи). При этом ее качество остается допустимым для пользователя, но цифровая подпись работать не будет. Получатель не сможет отличить истинное, хотя и несколько искаженное сообщение, от ложного. Кроме того, мультимедийные данные могут быть преобразованы из одного формата в другой. При этом традиционные средства защиты целостности работать также не будут. Можно сказать, что ЦВЗ способны защитить именно содержание аудио-, видеосообщения, а не его цифровое представление в виде последовательности бит. Кроме того, важным недостатком цифровой подписи является то, что ее легко удалить из заверенного ею сообщения, после чего приделать к нему новую подпись. Удаление подписи позволит нарушителю отказаться от авторства, либо ввести в заблуждение законного получателя относительно авторства сообщения. Система ЦВЗ проектируется таким образом, чтобы исключить возможность подобных нарушений.

Стегосистема может быть рассмотрена как система связи.

Алгоритм встраивания ЦВЗ состоит из трех основных этапов:

1) генерации ЦВЗ,

2) встраивания ЦВЗ в кодере

3) обнаружения ЦВЗ в детекторе.

1) Пусть W^*, K^*, I^*, B^* есть множества возможных ЦВЗ, ключей, контейнеров и скрываемых сообщений, соответственно. Тогда генерация ЦВЗ может быть представлена в виде

$$F:\ I^* \times K^* \times B^* \to W^*,\quad W = F(I, K, B),$$

где W, K, I, B - представители соответствующих множеств. Вообще говоря, функция F может быть произвольной, но на практике требования робастности ЦВЗ накладывают на нее определенные ограничения. Так, в большинстве случаев, $F(I, K, B) \approx F(I + \varepsilon, K, B)$, то есть незначительно измененный контейнер не приводит к изменению ЦВЗ. Функция F обычно является составной:

$$F = T \circ G,$$ где $G: K^* \times B^* \to C^*$ и $T: C^* \times I^* \to W^*$,

то есть ЦВЗ зависит от свойств контейнера, как это уже обсуждалось выше в данной главе. Функция G может быть реализована при помощи криптографически безопасного генератора ПСП с K в качестве начального значения.

Для повышения робастности ЦВЗ могут применяться помехоустойчивые коды, например, коды БЧХ, сверточные коды [9]. В ряде публикаций отмечены хорошие результаты, достигаемые при встраивании ЦВЗ в области вейвлет-преобразования с использованием турбо-кодов. Отсчеты ЦВЗ принимают обычно значения из множества $\{-1, 1\}$, при этом для отображения $\{0, 1\} \to \{-1, 1\}$ может применяться двоичная относительная фазовая модуляция (BPSK).

Оператор T модифицирует кодовые слова C^*, в результате чего получается ЦВЗ W^*. На эту функцию можно не накладывать ограничения необратимости, так как соответствующий выбор G уже гарантирует необратимость F. Функция T должна быть выбрана так, чтобы незаполненный контейнер I_0, заполненный контейнер I_W и незначительно модифицированный заполненный контейнер I'_W порождали бы один и тот же ЦВЗ:

$$T(C, I_0) = T(C, I_W) = T(C, I'_W),$$

то есть она должна быть устойчивой к малым изменениям контейнера.

2) Процесс встраивания ЦВЗ $W(i, j)$ в исходное изображение $I_0(i, j)$ может быть описан как суперпозиция двух сигналов:

$$\varepsilon:\ I^* \times W^* \times L^* \to I_W^*,\quad I_W(i, j) = I_0(i, j) \oplus L(i, j) W(i, j) p(i, j),$$

где $L(i,j)$ – маска встраивания ЦВЗ, учитывающая характеристики зрительной системы человека, служит для уменьшения заметности ЦВЗ; $p(i,j)$ – проектирующая функция, зависящая от ключа; знаком $\oplus$ обозначен оператор суперпозиции, включающий в себя, помимо сложения, усечение и квантование.

Проектирующая функция осуществляет «распределение» ЦВЗ по области изображения. Ее использование может рассматриваться, как реализация разнесения информации по параллельным каналам. Кроме того, эта функция имеет определенную пространственную структуру и корреляционные свойства, использующиеся для противодействия геометрическим атакам.

Для повышения защищенности файлов предлагается подписывать весь контейнер (электронный документ или объект авторского права) с внедренными ЦВЗ и электронной цифровой подписью, полученной с использованием закрытого ключа автора документа. Подпись должна храниться в удостоверяющем центре (УЦ).

Каждый легальный пользователь может с помощью открытого ключа (все они хранятся в УЦ в открытом доступе) проверить подлинность и неизменность файла. Цифровой водяной знак служит гарантией того, что даже если злоумышленник подпишет файл от своего имени, результаты проверки его электронной подписи и ЦВЗ не совпадут и можно будет установить нарушение. ЦВЗ выступает в качестве дополнительного уровня защиты, который иногда затруднительно даже обнаружить, а тем более обойти. Этот уровень защиты позволяет доказать авторство при экспертизе.

В ходе экспериментальной проверки использования одновременно нескольких технических мер защиты (ЦВЗ, ЭЦП и метки времени) значительно был получен результат, который позволяет предполагать повышение уровня защищенности электронного документа в системе при условии организации и использования такой защиты.

Список литературы: **1.** *Schneier B.* Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd ed. New York // John Wiley and Sons, **2.** *Шеннон К.*Работы по теории информации и кибернетики / Пер. с англ. –М.: Иностранная литература, 1963. – 829с. **3.** Системы защиты электронной информации на основе стеганографических алгоритмов [Текст] // Сборник научных трудов по материалам международной научно-практической конференции «Современные проблемы и пути их решения в науке, транспорте, производстве и образовании `2009». *[Коленко В.В., Нарожный А.В., Носов П.С.]* – Одесса:Черноморье. – 2009.