Виталий Григорьевич Иваненко, Никита Владиславович Ушаков
Национальной исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, г. Москва, 115409 , Россия
e-mail:VGIvanenko@mephi.ru, ORCID 0000-0003-0823-5501;
e-mail: u.nick@inbox.ru, ORCID 0000-0001-7347-239X

ЦИФРОВЫЕ ВОДЯНЫЕ ЗНАКИ В ЭЛЕКТРОННОМ ДОКУМЕНТООБОРОТЕ

DOI: http://dx.doi.org/10.26583/bit.2017.3.04

Аннотация. В данной статье рассматриваются существующие методы защиты электронных документов, отмечается их главные преимущества и недостатки. Анализируются основные угрозы для электронных документов, способы защиты. Исследуются недостатки ЭЦП, описываются методы их устранения. Описываются различные современные методы внедрения информации в электронные документы, выделяется два типа методов. Проводится сравнительный анализ данных методов встраивания цифровых водяных знаков в электронные документы. По итогам анализа выбран наиболее эффективный метод – метод обратимого сокрытия данных. Отмечается, что данный метод лучше всего использовать для обеспечения целостности и ЦВЗ и контейнера. Система встраивания ЦВЗ должна предотвращать попытки злоумышленников изменять ЦВЗ и исходные данные в контейнере. Приводятся требования к ЦВЗ, встраиваемому для защиты электронных документов. Описываются основные атаки на документ в формате PDF. Изучаются современные алгоритмы обратимого сокрытия данных. Рассмотрена правовая база защиты авторских прав. Перечисляются особенности использования ЦВЗ, а также других технических средств защиты в России. Отмечается, что в настоящее время использовать ЦВЗ как основное средство защиты электронных документов не представляется возможном, в связи с законодательством России. ЦВЗ используется в качестве дополнительного уровня защиты, о котором злоумышленнику обычно не известно. При встроенном ЦВЗ злоумышленник не сможет присвоить себе авторство над документом, даже если подпишет его от своего имени, ведь результаты проверки ЭЦП и ЦВЗ не совпадут. Делается вывод, что ЦВЗ могут служить эффективным дополнительным средством защиты электронных документов.

Ключевые слова: цифровые водяные знаки, цифровая подпись, электронные документы, встраивание информации, обратимый метод сокрытия данных

Для цитирования. **ИВАНЕНКО, Виталий Григорьевич; УШАКОВ, Никита Владиславович.** ЦИФРОВЫЕ ВОДЯНЫЕ ЗНАКИ В ЭЛЕКТРОННОМ ДОКУМЕНТООБОРОТЕ. Безопасность информационных технологий, [S.l.], v. 24, n. 3, p. 37-42, july 2017. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/262>. Дата доступа: 01 dec. 2017. doi:http://dx.doi.org/10.26583/bit.2017.3.04.

Vitaliy Grigorievich Ivanenko, Nikita Vladislavovich Ushakov
National Research Nuclear University "MEPhI",
Kashirskoe shosse, 31, Moscow, 115409, Russia
e-mail: VGIvanenko@mephi.ru, ORCID 0000-0003-0823-5501;
e-mail: u.nick@inbox.ru, ORCID 0000-0001-7347-239X

Digital watermarks in electronic document circulation

DOI: http://dx.doi.org/10.26583/bit.2017.3.04

Abstract. This paper reviews different protection methods for electronic documents, their good and bad qualities. Common attacks on electronic documents are analyzed. Digital signature and ways of eliminating its flaws are studied. Different digital watermark embedding methods are described, they are divided into 2 types. The solution to protection of electronic documents is

based on embedding digital watermarks. Comparative analysis of this methods is given. As a result, the most convenient method is suggested – reversible data hiding. It's remarked that this technique excels at securing the integrity of the container and its digital watermark. Digital watermark embedding system should prevent illegal access to the digital watermark and its container. Digital watermark requirements for electronic document protection are produced. Legal aspect of copyright protection is reviewed. Advantages of embedding digital watermarks in electronic documents are produced. Modern reversible data hiding techniques are studied. Distinctive features of digital watermark use in Russia are highlighted. Digital watermark serves as an additional layer of defense, that is in most cases unknown to the violator. With an embedded digital watermark, it's impossible to misappropriate the authorship of the document, even if the intruder signs his name on it. Therefore, digital watermarks can act as an effective additional tool to protect electronic documents.
Keywords: digital watermarks, digital signature, electronic documents, embedding information, reversible data hiding.
For citation. **IVANENKO, Vitaliy Grigorievich; USHAKOV, Nikita Vladislavovich.** Digital watermarks in electronic document circulation. IT Security, [S.l.], v. 24, n. 3, p. 37-42, july 2017. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/262>. Date accessed: 01 dec. 2017.
doi:http://dx.doi.org/10.26583/bit.2017.3.04.

В последние годы, как в государственных, так и коммерческих организациях все шире используется электронный документооборот, в связи с чем проблема защиты электронных документов является весьма актуальной. Очевидно, что в зависимости от своего содержания электронные документы имеют различную степень конфиденциальности. Существует также проблема подлинности документов, передаваемых в сети, например, документ, полученный по электронной почте, нельзя удостоверить печатью или подписать обычным способом. Поэтому электронный документооборот необходимо сопровождать различными организационными и техническими мерами и средствами для защиты электронных документов от несанкционированного доступа или модификации.

Угрозы для электронных документов являются типичными для информации в электронном виде – это угрозы целостности, конфиденциальности и доступности [1]. Для противодействия типовым угрозам при использовании электронного документооборота должна также обеспечиваться сохранность документов от потери и порчи и иметься возможность их быстрого восстановления. К примеру, системы электронного документооборота, в основе своей использующие базы данных Microsoft SQL Server или Oracle, используют средства резервного копирования, встроенные в эти базы данных.

Безопасный доступ к данным внутри системы электронного документооборота обеспечивается аутентификацией и разграничением прав пользователя. Наиболее распространены два метода аутентификации – парольный и имущественный [2]. На парольный метод сильно влияет человеческий фактор – пароль часто оказывается известен нарушителю. Имущественный метод предоставляет большую степень защиты, для аутентификации необходимы различные USB-ключи, смарт-карты и т.д. Данный метод тоже не защищен от человеческого фактора, однако, кроме пароля необходимо иметь и устройство для доступа. В любой системе обязательно должно быть предусмотрено разграничение прав пользователя, и чем гибче и детальнее, тем лучше.

Конфиденциальность чаще всего обеспечивается криптографическими методами. С помощью них конфиденциальность сохраняется даже при попадании документа в руки злоумышленников. С криптографическими средствами следует обращать внимание и на организационную составляющую защиты информации. Вне зависимости от криптографических методов, нарушитель может получить доступ к документу при помощи компьютера с открытым на нем документом. Расшифровка информации также не представляет труда, если не осуществляется контроль ключей у пользователей.

Электронно-цифровая подпись (ЭЦП) является основным средством для обеспечения подлинности документа, полученного в электронном виде. ЭЦП служит для защиты документа от искажения, подмены авторства, отказа от авторства. Электронно-цифровая подпись по сути является цифровой печатью, потому что, в отличие от физической подписи, она является общей для предприятия, отдела или компьютера. Получается, что любой человек, имеющий доступ к ресурсам, отвечающим за создание и другие действия с ЭЦП, может совершить следующие противоправные действия:

- изменить исходный документ, после чего сгенерировать новую ЭЦП;
- изменить авторство документа, в итоге присвоив себе чужой документ, или отправить свой документ под чужим именем;
- уничтожить исходный документ, отправить другой документ вместо исходного.

Таким образом, из-за таких нарушителей под угрозой оказывается не только целостность документа, но также и авторство. Для защиты документа от подобного рода воздействий рекомендуется использовать помимо ЭЦП и другие средства, фактически объединяя криптографические и стеганографические методы защиты.

Одним из таких средств может служить цифровой водяной знак (ЦВЗ) – специальная метка, встраиваемая в контейнер с целью защиты авторских прав и подтверждения целостности контента [3]. ЦВЗ применяются для защиты от несанкционированного использования и копирования документов, с помощью ЦВЗ возможно отследить нарушителя, создающего неправомерные копии [4]. Система встраивания ЦВЗ должна предотвращать попытки злоумышленников изменять цифровой водяной знак и исходные данные в контейнере.

Существует множество различных методов встраивания ЦВЗ в документы. Их классификация приведена в работе [5], где рассматриваются различные типы цифровых водяных знаков: видимые, невидимые, считываемые из документа или нет, устойчивые, полу устойчивые, хрупкие. Для увеличения устойчивости, а также размера ЦВЗ текст должен иметь как можно большую длину. Кроме этого, встраивания ЦВЗ в текст зависит также от языка, грамматики, стилей написания и т.д. Можно выделить две категории методов встраивания цифровых водяных знаков в электронные документы: встраивающие напрямую в текст и встраивающие в текст в виде изображения (документы формата PDF). К первой категории относятся синтаксические методы, семантические методы, структурные методы [6].

Синтаксические методы основываются на использовании синтаксических трансформаций для внедрения бита ЦВЗ [7]. В результате операций над текстом часто содержания документа сильно меняется, из-за чего текст перестает отражать оригинальное послание автора. Кроме того, использовать данный подход возможно только на длинных текстах.

Семантические методы фокусируются на использовании семантический структура текста для внедрения цифрового водяного знака. Глаголы, существительные, предлоги, написание слов, акронимы, структуры предложения, грамматические правила и т.д. – всё это используется для ЦВЗ [8] Однако всё вышеперечисленное зависит от языка и имеет ограниченную применимость. Недостатком данного подхода является, как и для предыдущего метода, визуальное изменение электронного документа.

Структурные методы концентрируются на изменении структуры текста. Здесь ЦВЗ встраивается за счет использование невидимых символов Unicode. Стандарт Unicode предоставляет множество различных пробелов. В отличие от предыдущих методов, структурный сохраняет исходное содержимое текста, однако этот метод не сохраняет длину текста и может использоваться не со всеми типами текстовых документов.

Наиболее перспективным методом, встраивающим ЦВЗ в электронный документ формата PDF, является метод обратимого сокрытия данных (RDH, reversible data hiding) [9]. Он используется для обеспечения целостности и ЦВЗ и контейнера. Его суть

заключается в том, что ЦВЗ представляет из себя информацию о частях, которые были изменены при встраивании, поэтому при извлечении данных контейнер можно привести к исходному виду. Кроме этого, таким методом также проверяется, проводились ли какие-либо изменения над исходным контейнером после внедрения ЦВЗ. В работах [10] и [11] предлагается новый алгоритм RDH, суть которого состоит в том, что исходное изображения делится на непересекающиеся блоки n пикселей. После этого генерируется n-размерная гистограмма при помощи вычисления частоты пиксель-значения-массив размером n в каждом отдельном блоке. Цифровой же водяной знак внедряется при помощи модификации получившейся гистограммы.

Таким образом, для электронных документов в текстовом формате рекомендуется использовать структурные методы, для документов в формате PDF (portable document format) метод обратимого сокрытия данных.

ЦВЗ используется в качестве дополнительного уровня защиты, о котором чаще всего злоумышленнику не известно [12]. При встроенных цифровых водяных знаках злоумышленник не сможет присвоить себе авторство над файлом, даже если подпишет его от своего имени, ведь результаты проверки ЭЦП и ЦВЗ в таком случае не совпадут.

ЦВЗ должен быть невидим для того, чтобы злоумышленник не имел возможности визуально его обнаружить [13]. Для большей устойчивости к атакам ЦВЗ следует распределить по всему цифровому контейнеру. Если речь идет об изображении (фотографии), то основными атаками (методами уничтожения) на ЦВЗ могут являться масштабирование, вырезание каких-либо участков изображения, поворот на произвольный угол, конвертирование в другой графический формат и т.д. Для защиты контента цифровой водяной знак должен успешно противостоять этим атакам.

Авторские права регулируются Гражданским кодексом Российской Федерации и защищаются Уголовным кодексом и Кодексом об административных нарушениях [14].

Основной законодательный акт, регулирующий авторские и исключительные права на произведение — это четвертая часть Гражданского Кодекса Российской Федерации [14]. Она полностью посвящена правам на результаты интеллектуальной деятельности и средства индивидуализации.

Наибольшее значение технические средства защиты имеют при распространении произведений через Интернет. При выкладывании своей работы в сеть Интернет считается, что произведение доведено до всеобщего сведения. То есть, согласно статье 1270 ГК, автор использует исключительное право на использование своего произведения. При этом, вне зависимости от места и времени, кто угодно может получить доступ к графической работе. Однако, часто такие объекты авторского права размещаются в Интернете без ведома и согласия автора. Для предотвращения таких случаев произведения должны обеспечиваться техническими средствами защиты перед их публикацией в Интернете или других сетях передачи данных [15]

Заключение

Согласно ст. 1299 части 4 ГК РФ, техническими средствами защиты авторских прав признаются любые технологии, технические устройства или их компоненты, контролирующие доступ к произведению, предотвращающие либо ограничивающие осуществление действий, которые не разрешены автором или иным правообладателем в отношении произведения. В соответствии со статьей 1300 ГК РФ автор обладает правами и на документ с внедренным ЦВЗ. Однако, из-за отсутствия законодательной базы о цифровых водяных знаках использовать их в полной мере как доказательство авторства не представляется возможным, потому что трактовка статьи 1299 ГК РФ может и не рассматривать ЦВЗ как технические средства защиты авторского права. Следовательно, ЦВЗ в настоящее время в РФ можно использовать лишь для обнаружения источника утечки документов или для подтверждения целостности документа.

Цифровые водяные знаки являются перспективным методом защиты информации, при создании нормативных документов возможно будет использование ЦВЗ не только для обнаружения нарушителя, но и как доказательство авторства.

СПРИСОК ЛИТЕРАТУРЫ:

1 Гладких А.А., Дементьев В.Е. Базовые принципы информационной безопасности вычислительных систем, Ульяновск: УлГТУ, 2009.
2 Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография: Салон-Пресс Стратегия развития информационного общества в РФ, 2009.
3 Иваненко В.Г., Ушаков Н.В. Встраивание цифровых водяных знаков в видеозаписи. Безопасность информационных технологий, 2016, №4, с. 21-24.
4 Иваненко В.Г., Лапшин А.И. Встраивание цифровых водяных знаков методом изменения времени задержки эхо сигнала. Безопасность информационных технологий , 2016, №1, с.50-52.
5 An Existential Review on Text Watermarking Techniques International Journal of Computer Applications (0975 – 8887) Volume 120 –No.1 June 2015, p. 29-32
6 Stefano Giovanni Rizzo, Flavio Bertini, Danilo Montesi Text Authorship Verification through Watermarking 2016 European Intelligence and Security Informatics Conference, p.168-171.
7 N. Mir. Copyright for web content using invisible text watermarking. Computers in Human Behavior, Volume 30, p. 648–653, January2014.
8 S. Hosmani, H. R. Bhat, and K. Chandrasekaran. Dual stage text steganography using unicode homoglyphs, Security in Computing and Communications, p. 265–276. Springer, 2015.
9 Znicheng Ni, Yun-Qing Shi, Nirwan Asari, Wei Su. Reversible data hiding IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 16, NO. 3, MARCH 2006, p.345-362.
10 Nice Mathew, A. Grace Selvarani, A Novel Reversible Data Hiding Technique based on Histogram Shifting and Efficient use of Location Map International Journal of Computer Applications (0975 – 8887) Volume 89 – No.1, March 2014, с. 25-29.
11 Pawar P. H., Jondhale K. C. 2012 Histogram-based reversible data hiding using block division. In: 2012 IEEE international conference on advanced communication control and computing technologies (ICACCCT), p.295–299.
12 Иваненко В.Г., Родченко С.В. Встраивание цифровых водяных знаков в аудиосигналы. Безопасность информационных технологий, 2011, №1, с.94-95.
13 Иваненко В.Г., Шабаева Я.Р., Защита изображений от модификации с помощью замены наименее значащих бит. Безопасность информационных технологий, 2013, №1, с. 103-104.
14 Кодексы и Законы Российской Федерации. Правовая навигационная система. http://www.zakonrf.info/
15 Коханович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. К:МК-Пресс, 2006.

REFERENCES:

[1] Gladkih A.A., Dementyev V.E. Basic principles of information security in computing systems, Ul'yanovsk: ULGTU, 2009 (in Russian).
[2] Gribunin V.G., Okov I.N., Turincev I.V. Digital steganography: Salon-Press Strategiya razvitiya informacionnogo obshchestva v RF, 2009. (in Russian).
[3] Ivanenko V.G., Ushakov N.V. Digital video watermarking. Bezopasnost' informacionnyh tekhnologij, 2016, №4, p. 21-24 (in Russian).
[4] Ivanenko V.G., Lapshin A.I. Inserting digital watermarks by method on delaying echo. Bezopasnost' informacionnyh tekhnologij, 2016, №1. (in Russian).

[5] An Existential Review on Text Watermarking Techniques International Journal of Computer Applications (0975 – 8887) Volume 120 –No.1 June 2015, p. 29-32.
[6] Stefano Giovanni Rizzo, Flavio Bertini, Danilo Montesi Text Authorship Verification through Watermarking 2016 European Intelligence and Security Informatics Conference, p.168-171.
[7] N. Mir. Copyright for web content using invisible text watermarking. Computers in Human Behavior, Volume 30, p. 648–653, January2014.
[8] S. Hosmani, H. R. Bhat, and K. Chandrasekaran. Dual stage text steganography using unicode homoglyphs, Security in Computing and Communications, p. 265–276. Springer, 2015.
[9] Znicheng Ni, Yun-Qing Shi, Nirwan Asari, Wei Su. Reversible data hiding IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 16, NO. 3, MARCH 2006, p.345-362.
[10] Nice Mathew, A. Grace Selvarani, A Novel Reversible Data Hiding Technique based on Histogram Shifting and Efficient use of Location Map International Journal of Computer Applications (0975 – 8887) Volume 89 – No.1, March 2014, p. 25-29.
[11] Pawar P. H., Jondhale K. C. 2012 Histogram-based reversible data hiding using block division. In: 2012 IEEE international conference on advanced communication control and computing technologies (ICACCCT), p.295–299.
[12] Ivanenko V.G., Rodchenko S.V. Digital watermarks embedding in audio signals. Bezopasnost' informacionnyh tekhnologij, 2011, №1, p.94-95 (in Russian).
[13] Ivanenko V.G., Shabaeva Y.R., Image protection from modification using less significant bit method. Bezopasnost' informacionnyh tekhnologij, 2013, №1, p. 103-104 (in Russian).
[14] Codes and Laws of Russian Federation. Legal navigational system. http://www.zakonrf.info/ (in Russian).
[15] Kohanovich G.F., Puzyrenko A.Ju. Computer steganography. Teorija i praktika. K:MK-Press, 2006. (in Russian).