Технология измерения биометрических параметров автора важных бумажных документов и их использование для защиты документов от подделок и фальсификации

А. М. Алюшин
Федеральное государственное автономное образовательное учреждение высшего образования
«Национальный исследовательский ядерный университет «МИФИ»
alyshin@list.ru

***Аннотация*. Для защиты важных юридических, либо финансовых документов от их возможных фальсификаций и подделок предлагается в дополнение к обычной подписи автора использовать так называемую речевую подпись (РП). С полиграфической точки зрения РП представляет собой фрагмент изображения, который может быть распечатан на бумажном носителе документа, в частности, он может быть встроен в рамку документа. Вышеупомянутое изображение представляет собой сонограмму, включающую информацию как о содержимом всего документа, либо его самой важной части, так и персональную биометрическую информацию. При этом статическая биометрическая информация используется для идентификации личности автора, а динамическая – для фиксации психоэмоционального состояния автора при визировании документа, что позволяет выявлять неправомерные случаи визирования документов под нажимом.**

Ключевые слова: измерение статических и динамических биопараметров; защита документов; речевая подпись

I. Введение

Мы живем в мире высоких информационных технологий, где значительная часть операций связана в той или иной степени с компьютером. Но, несмотря на это, объемы документооборота в его классической форме с использованием бумажного носителя не становятся меньше. Это означает, что вопросы, связанные с защитой документов как в бумажном, так и в цифровом виде, не потеряли своей актуальности. Существующие и возникающие информационные угрозы лишь подчеркивают все возрастающую роль инновационных технологий для защиты документов от подделок.

Целью исследования является разработка технологии речевой подписи как одного из инновационных способов защиты документов от подделок.

Работа выполнена в рамках конкурсной части госзадания НИЯУ МИФИ на 2017-2019 гг., проект №25.2911.2017/4.6

II. Существующие методы защиты документов

В табл. 1 представлены результаты анализа наиболее значимых технологий, применяемых для защиты бумажных и электронных документов в настоящее время . К небиометрическим методам защиты отнесено использование водяных знаков, голограмм, специальной бумаги, защитных волокон.

ТАБЛИЦА I Технологии защиты документов

Метод защиты	**Основные недостатки существующих методов защиты**	
	Бумажный документооборот	***Электронный документооборот***
Использование личной подписи	Метод не защищает текст документа и не защищает саму подпись от подделки	Метод не защищает ни авторство документа, ни сам текст от подделки
Использование отпечатков пальцев	Метод не является распространенным, так как сложен и неудобен в реализации на практике. Не защищает текст документа.	Метод не защищает ни авторство документа, ни сам текст от подделки.
ЭЦП (электронно-цифровая подпись)	Данный метод для защиты бумажных документов не используется	Защита авторства документа является спорной
Небиомет-рические методы защиты	Не является распространенным методом защиты документов. Не защищает авторство документа	Данный метод для защиты электронных документов на практике не используется

Основным наиболее распространенным методом подтверждения авторства на сегодняшний день является использование личной подписи. Однако применительно к бумажным документам этот метод не защищает ни текст документа, ни саму подпись от подделок. Применительно к электронному документообороту метод не защищает ни авторство документа, ни сам текст от подделок.

Использование отпечатков пальцев является достаточно надежным методом защиты в случае

использования бумажных документов. Однако основным недостатком метода является сложность и неудобство его технической реализации на практике. В случае использования электронных документов метод не защищает ни авторство документа, ни сам текст от подделок.

Определенный интерес представляет собой технология ЭЦП [1–4]. Основной алгоритм ее применения на практике следующий:

1. Автор (Пользователь А) вычисляет Хэш-функцию (ХФ) документа.
2. Используя алгоритм шифрования RSA, Пользователь А создает зашифрованную ХФ (ЗХФ), используя закрытый ключ.
3. Пользователь А отправляет сам документ, ЗХФ и открытый ключ для расшифровки другому человеку (Пользователь В). В итоге, Пользователь В (или злоумышленник, если ему удалось перехватить сообщение) имеет у себя сам документ, ЗХФ и открытый ключ (открытый ключ может не передаваться, он просто может быть доступен всем в открытым виде).
4. Пользователь В считывает ЗХФ документа и расшифровывает ее, используя открытый ключ.
5. В итоге осуществляется проверка этих двух ХФ на совпадение. Несовпадение функций однозначно свидетельствует об изменении документа.

Злоумышленник, которому удалось перехватить сообщение, тоже может проделать все эти действия. Однако внести изменения у него не получится, так как при этом поменяется ХФ. Создание же новой ЗХФ невозможно без обладания закрытым ключом.

Общая схема использования технологии ЭЦП приведена на рис. 1.

Уязвимость технологии ЭЦП обусловлена наличием трех следующих критических факторов:

- возможность взлома закрытого ключа с помощью современных высокопроизводительных компьютеров;
- неправильно построенный алгоритм вычисления ХФ позволит создать два разных текста с одинаковой ХФ;
- возможность кражи закрытого ключа.

В настоящее время разработаны достаточно эффективные алгоритмы вычисления ХФ, которые позволяют минимизировать негативное влияние первых факторов. Вопрос, связанный с хранением и защитой закрытого ключа, представляет самую большую угрозу в безопасности данной технологии и криптографии в целом.

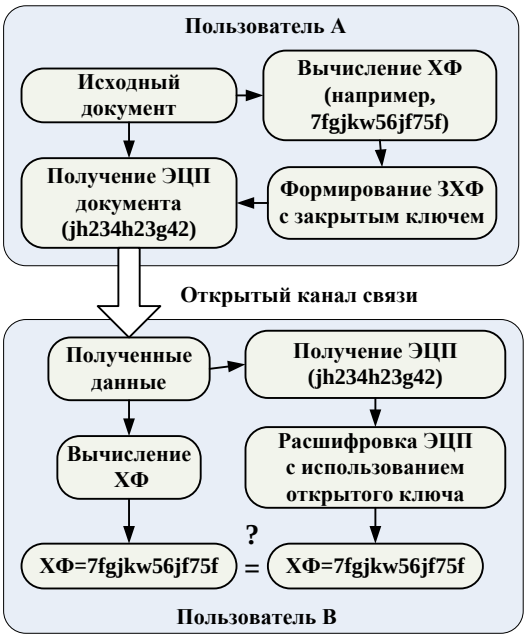

Рис. 1. Технология ЭЦП

К сожалению, применяемые на практике дополнительные устройства, которые хранят закрытый ключ например, смарт-карты, токены, usb-брелки и др., не могут решить эту проблему на принципиальном уровне.

III. Технология речевой подписи

Исходя из вышесказанного, а также из анализа существующих технологий защиты документов можно сделать следующий вывод. Ни одна из существующих технологий защиты документов не связывает текст документа, авторство документа с биометрическими данными человека. Именно поэтому наиболее идеальной технологией будет являться такая технология, которая бы связала защиту документа с биометрическими данными человека. Такой подход позволит исключить какие-либо несанкционированные изменения в документе без автора данного документа. Наиболее близкой к такой технологии является технология РП [5–6, 11].

Сущность данной технологии заключается в следующем. В конец или любое другое место защищаемого документа добавляется изображение спектрограммы речевого сигнала, которое и является РП [7–10]. В данном фрагменте хранится некоторая важная информация, связанная с защищаемым документом таким образом, что изменение основной части текста повлечет за собой изменение РП. При этом сделать это без автора этого документа невозможно. Под важной информацией подразумеваются данные, которые подчеркивают основные аспекты документа, такие как, например: сумма договора, обязанности сторон, сроки, координаты, телефоны, номера счетов и т.д. Общая схема использования данной технологии представлена на рис. 2.

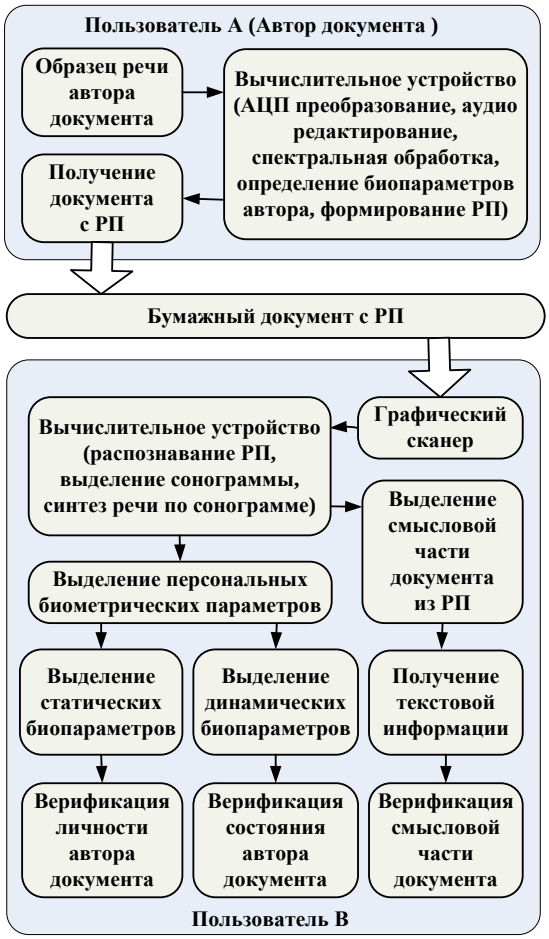

Рис. 2. Схема использования технологии РП

Технология РП позволяет использовать в качестве вычислительных устройств широкий спектр современных образцов персональных компьютеров, смартфонов и сотовых телефонов.

Передача в составе РП биометрической информации является дополнительным уровнем защиты документа от фальсификаций и подделок. Биометрические параметры, передаваемые в составе РП, подразделены на две группы – статические и динамические.

Первая группа биопараметров предназначена для осуществления верификации личности автора документа. Типичными представителями биопараметров данной группы являются:

- значения формантных частот речеобразующего тракта автора документа;
- тембр голоса (число и амплитуда обертонов формантных частот).

Вторая группа биопараметров позволяет осуществить контроль состояния автора документа в момент его подписания. К этой группе относятся биопараметры, которые в значительной степени подвержены существенным изменениям в соответствии с текущим уровнем нервного напряжения, стресса, страха. Типичными представителями второй группы являются:

- относительный уровень тремора в голосе автора документа в его нормальном физическом и психоэмоциональном состоянии;
- уровень модуляции речевой информации сердечной и дыхательной активностью в нормальном состоянии;
- число сердечных сокращений и вариабельность сердечного ритма в нормальном состоянии.

Биопараметры первой и второй групп определяются на основе обработки спектральной информации автора документа. Для этой цели при проведении данного исследования было разработано специализированное программное обеспечение. Наиболее эффективно применение рассмотренной технологии для защиты документооборота между известными партнерами. В этом случае статические и динамические (для нормального состояния) биопараметры сторон заносятся в локальные базы данных. Для определения динамических биопараметров необходимо использовать специализированные приложения, устанавливаемые на тот, либо иной вид вычислительной, в первую очередь, мобильной техники.

Объем передаваемых в составе РП данных может варьироваться в достаточно широком диапазоне. Так, в минимальном варианте, РП может представлять собой сонограмму, кодирующую цифровую информацию о статических и динамических биопараметрах автора документа, например, с помощью тональных сигналов. Это дает возможность использовать унифицированные средства кодировки и декодировки спектральной информации.

РП может содержать сонограмму достаточно продолжительного речевого сообщения автора. В этом случае временная продолжительность сонограммы достаточна для точного определения статических и динамических биопараметров автора на стороне Пользователя В.

В оптимальном варианте, изображение, содержащее РП, имеет размер порядка 100x5000 пикселей. В этом случае оно, как правило, содержит две части. Первая часть кодирует цифровые данные о биопараметрах автора. Вторая часть передает его натуральное речевое сообщение.

На рис. 3 представлен типичный пример графического изображения РП оптимального размера, соответствующего одному предложению. Графическое изображение РП для представленного примера содержит также ряд маркерных линий, расположенных сверху и снизу изображения сонограммы. Данные графические элементы предназначены для быстрого и надежного распознавания РП на документе.

На представленном примере хорошо видна периодическая структура сонограммы, соответствующая обертонам (гармоникам) основных формантных частот

говорящего. Число и мощность (яркость) присутствия в голосе данных компонентов, как было упомянуто выше, является отличительными признаками автора, которые используются в качестве передаваемых в составе РП индивидуальных биопараметров.

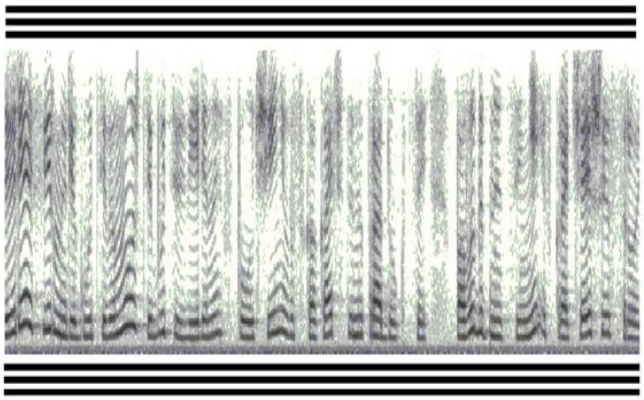

Рис. 3. Примеры РП в составе документа

IV. Сравнение РП с другими методами защиты документов

Основными достоинствами рассмотренной технологии РП по сравнению с другими применяемыми на практике методами (табл. 1) являются возможности:

- осуществить защиту авторства документа, представленного как в бумажном, так и в электронном виде;
- выявлять случаи составления документов под физическим, либо психическим давлением;
- реализовать технологию практически на всех типах современных стационарных и мобильных устройств.

V. Заключение

Предложенная технология защиты документов с помощью РП является универсальной и может быть использована как самостоятельно, так и совместно с другими методами защиты документов.

Разработаны специализированные приложения, реализующие функции РП, для смартфонов с ОС Android. Показана возможность установки и эффективной работы таких приложений на смартфонах с камерами невысокой разрешающей способности и процессорами с тактовыми частотами порядка 600 Mhz.

Проведена экспериментальная лабораторная апробация предложенной технологии. Достоверность передачи персональной биоинформации в случае многократного копирования бумажных документов с РП составляет не менее 85–95%.

Список литературы

[1] Rath T., Manmatha R. Word image matching using dynamic time warping // Proc. IEEE Conf. Computer Vision and Pattern Recognition, 2003. Vol. 2. P. 521-527.

[2] Zhu G., Zheng Y., Doermann D., Jaeger S. Multi-Scale structural saliency for signature detection // Proc. IEEE Conf. Computer Vision and Pattern Recognition. 2007. P. 1-8.

[3] Fang B., Leung C.H., Tang Y.Y., Tse KW., Kwok P.C.K., Wong Y.K. Off-Line signature verification by the tracking of feature and stroke positions // Pattern Recognition. 2003. Vol. 36. No. 1. P. 91-101. DOI: 10.1016/S0031-3203(02)00061-4

[4] Zheng Y., Li H., Doermann D. Machine printed text and hand writing identification in noisy document images // IEEE Trans. Pattern Analysis and Machine Intelligence. 2004. Vol. 26. No. 3. P. 337-353. DOI: 10.1109/TPAMI.2004.1262324

[5] Li Y., Zheng Y., Doermann D., Jaeger S. Script independent text line segmentation in freestyle handwritten documents // IEEE Trans. Pattern Analysis and Machine Intelligence. 2008. Vol. 30. No. 8. P. 1313-1329. http://doi.ieeecomputersociety.org/10.1109/TPAMI.2007.70792

[6] Secure Hash Standard (SHS). Federal information processing standards publication, FIPS PUB 180-4. 2015. 31 p.
http://dx.doi.org/10.6028/NIST.FIPS.180-4

[7] Дворянкин С.В. Речевая подпись. М. РИО. 2003, 184 с.

[8] Алюшин А.М., Дворянкин С.В. Использование речевых технологий для защиты документооборота //Безопасность информационных технологий. 2017. №2. С. 6-15.
DOI: http://dx.doi.org/10.26583/bit.2017.2.01

[9] Алюшин А.М., Дворянкин Н.С. Особенности распознавания изображений речевой подписи на мобильных устройствах //Безопасность информационных технологий. 2015. № 4. С. 38-45.

[10] Vorobiov V.I. Inter component phase processing of speech signals for their recognition and identification of announcers // XVIII Session of the Russian Acoustical Society, Taganrog, September 11-15, 2006. P. 529-523.

[11] Козлов Ю.Е. Подходы к определению надежности мультимодальной трехмерной динамической подписи // Безопасность информационных технологий. 2018. № 1. С. 74-80. DOI: http://dx.doi.org/10.26583/bit.2018.1.07