

Метод защиты PDF-документов от подделки с возможностью локализации изменений

П.М. Диканев¹, Ю.Д. Выборнова¹

¹Самарский национальный исследовательский университет им. академика С.П. Королева, Московское шоссе 34а, Самара, Россия, 443086

Аннотация

В статье предлагается новый метод защиты PDF-документов от подделки с возможностью локализации изменений. Метод основан на встраивании цифровых водяных знаков (ЦВЗ) в форме QR-кодов, кодирующих секретные сообщения. Уникальное бинарное изображение ЦВЗ (QR-код) встраивается в наименее значащие биты коэффициентов дискретного вейвлет-преобразования каждой страницы. Анализ извлеченных секретных сообщений позволяет обнаруживать и локализовать такие атаки как добавление, удаление и переупорядочивание страниц документа, при этом анализ самих встроенных изображений позволяет выявить подделку фрагмента на конкретной странице. Проведено экспериментальное исследование работоспособности метода. Согласно результатам экспериментов метод подходит для решения задач аутентификации PDF-документов, а также для стеганографической передачи сообщений.

Ключевые слова

Защита документов, PDF, цифровой водяной знак, аутентификация

1. Введение

В эпоху пандемии COVID-19 организации все чаще вынуждены обмениваться электронными скан-копиями собственноручно подписанных документов. Такие копии могут быть легко подделаны с помощью фоторедакторов.

Как правило, для защиты PDF-документов применяются цифровые подписи [1] или криптографические хеш-функции [2], однако, эти методы обеспечивают только защиту целостности и не позволяют определить, какие именно фрагменты были подделаны злоумышленником.

Для защиты авторских прав на PDF-документы могут применяться методы встраивания цифровых водяных знаков (ЦВЗ) в растровые изображения [3]. Однако, в задаче защиты подлинности PDF-документов такие методы недостаточно эффективны. Поскольку документы часто являются многостраничными, возникает необходимость обеспечить возможность доказать факт удаления страниц. Таким образом, каждая страница документа должна защищаться уникальным ЦВЗ, следовательно, встает вопрос защищенного хранения набора ЦВЗ. Такой набор может быть легко скомпрометирован злоумышленником и использован при подделке.

2. Предлагаемый метод защиты PDF-документов

В данной статье предлагается метод незаметного встраивания QR-кодов, которые не нужно хранить: аутентификация осуществляется по секретному сообщению, на основе которого был сгенерирован QR-код [4]. Для каждой страницы используется уникальный код, что позволит определить изменение порядка страниц документа. Секретное сообщение строится из номера страницы и криптографического ключа, обеспечивающего защиту от компрометации.

Процедура встраивания ЦВЗ заключается в замене наименее значащих битов LH-компоненты дискретного вейвлет-преобразования (ДВП) битами QR-кода [5].

3. Экспериментальные исследования

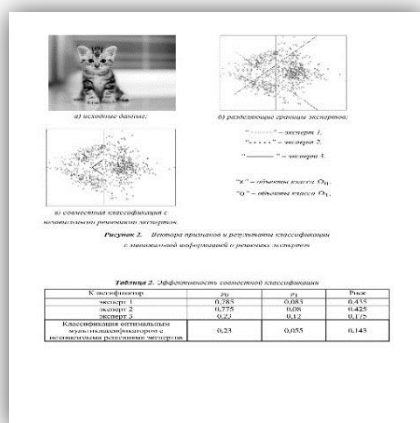
Проведено сравнение незаметности ЦВЗ при встраивании в разные уровни LH-компоненты ДВП: для защиты PDF-документов целесообразно использовать первый уровень.

Таблица 1

Исследование незаметности ЦВЗ при встраивании в разные уровни LH компоненты ДВП

	Уровень 1	Уровень 2	Уровень 3
MSE	28,03	97,54	112,22
PSNR	33,52	27,61	28,02

На Рисунке 1 приведен пример работы алгоритма при подделке страницы документа.



а)



б)

Рисунок 1: а) Страница с встроенным QR-кодом после подделки фрагмента. б) QR-код, извлечённый из страницы с подделанным фрагментом

4. Благодарности

Исследование выполнено при финансовой поддержке РФФИ в рамках научных проектов № 19-29-09045, № 19-07-00474, № 20-37-70053, № 19-07-00138.

5. Литература

- [1] Shaikhli, I.F. Protection of Integrity and Ownership of PDF Documents Using Invisible Signature / I.F. Shaikhli, A. Zeki, R. Makarim, A. Pathan // UKSim 14th International Conference on Computer Modelling and Simulation. – 2012. – P. 533-537.
- [2] Martín-Rodríguez, F. Scanned Documents Secure Authentication Based on Simple Watermarking / F. Martín-Rodríguez, J.M. Fernández-Montenegro // IEEE Carnahan Conference on Security Technology. – 2011. – P. 1-5.
- [3] Cardamone, N. DWT and QR Code Based Watermarking for Document DRM / N. Cardamone, F. d'Amore // Lecture Notes in Computer Science. – 2019. – Vol. 11378. – P. 137-150.
- [4] Библиотека создания QR-кодов [Электронный ресурс]. – Режим доступа: <https://pypi.org/project/qrcode> (02.07.2020).
- [5] Vybornova, Y. A New Watermarking Method for Video Authentication with Tamper Localization / Y. Vybornova // Lecture Notes in Computer Science. – 2020. – Vol. 12334. – P. 201-213.