

УДК 004.056.53

РАЗРАБОТКА МЕТОДА АУТЕНТИФИКАЦИИ PDF-ДОКУМЕНТОВ НА ОСНОВЕ ВСТРАИВАНИЯ QR-КОДОВ

© Диканев П.М.

*Самарский национальный исследовательский университет
имени академика С.П. Королева, г. Самара, Российская Федерация*

e-mail: dikanev.pavel@mail.ru

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.

Важным и актуальным стал вопрос защиты ценных документов, хранящихся и передаваемых от компьютера к компьютеру, от подделок и фальсификаций.

Как правило, для защиты PDF-документов применяются цифровые подписи или криптографические хеш-функции, 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. 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 [1; 2].

Целью работы стали разработка и реализация метода защиты и аутентификации PDF-документов на основе встраивания QR-кодов.

В качестве цифрового водяного знака для защиты было выбрано изображение, содержащее QR-код. Это двухмерный штрих-код. Он представляет собой набор черных квадратов, упорядоченных на квадратной сетке на белом фоне, и приспособлен для быстрого считывания и распознавания с помощью фотокамер. Им можно зашифровывать в удобном для чтения машиной формате различную информацию.

Разложение страницы для встраивания ЦВЗ осуществляется на HL-компоненте второго уровня вейвлет-преобразования (DWT). Это позволяет скрыть изменения контейнера изображения. Так как при изменении LL-экспоненты или при 1м уровне LH изменение изображения становится видно невооруженным глазом.

Количество слоев при встраивании в наименее значимые биты (LSB) было определено также опытным путем – 5. Такое количество позволяет встраивать и извлекать коды из цветных страниц документа с картинками, так как они наиболее распространены. Для ч/б текста же достаточно 3–4.

После извлечения кода было принято решение использовать пороговую и медианную фильтрацию, так как встраивание происходит всего лишь в 5 слоев кода, что необходимо для незаметности встраивания.

В дальнейшем планируется модернизировать систему, добавив шифрование секретного сообщения, что увеличит надежность данного метода.

Библиографический список

1. Altaay A.A.J., Sahib S.B., Zaman M. An introduction to image steganography techniques // International Conference on Advanced Computer Science Applications and Technologies (ACSAT). 2012. 122–126 с.
2. Федосеев В.А., Митекин В.А. Теоретические основы стеганографии и цифровых водяных знаков: учеб. пособие. Самара: Издательство Самарского университета. 2017. С. 1–24, 65–106.