Литература

1. Лавриченко, О.В. Управление инновационными системами промышленных предприятий и разработка модели их классификации / Лавриченко О.В. // Вестник Южно-Уральского государственного университета. Серия: Компьютерные технологии, управление, радиоэлектроника, 2014. Т. 14. № 4. С. 10.
2. Земцов А.Н., Болгов Н.В., Божко С.Н. Многокритериальный выбор оптимальной системы управления базы данных с помощью метода анализа иерархий // Инженерный вестник Дона, 2014, №2. URL: http://ivdon.ru/ru/magazine/archive/n2y2014/2360.
3. Земцов А.Н., Ньяти Р.С. Моделирование и оценка показателей надежности и отказоустойчивости систем связи // Инженерный вестник Дона, 2019, №4. URL: http://ivdon.ru/ru/magazine/archive/N5y2019/5995.
4. Земцов А.Н., Чан Зунг Хань. Анализ эффективности алгоритмов планирования передачи пакета в сетях LTE // Инженерный вестник Дона, 2019, №4. URL: http://ivdon.ru/ru/magazine/archive/n4y2019/5840.
5. Земцов А.Н., Чан Зунг Хань. О повышении доступности шлюза по умолчанию в корпоративных сетях // Инженерный вестник Дона, 2019, №9. URL: http://ivdon.ru/ru/magazine/archive/N9y2019/6243.

А.Н. Земцов, В.Ю. Цыбанов

РАЗРАБОТКА ПРОГРАММНЫХ СРЕДСТВ ДЛЯ ЗАЩИТЫ ИЗОБРАЖЕНИЙ МЕТОДАМИ ЦИФРОВОЙ СТЕГАНОГРАФИИ

(Волгоградский государственный технический университет)

В последние годы в Российской Федерации наметился переход от традиционного документооборота к системам с электронной формой представления документов, вызванный, в том числе, необходимостью организации дистанционного взаимодействия между различными структурными подразделениями, коммерческих предприятий и государственных учреждений, что позволило повысить их производительность [1], а также реализовать комплекс концептуальных подходов и методов к оптимизации этого процесса [2].

Задача защиты изображений была актуальна с момента появления изображений, но методы защиты изображений появились относительно недавно. Актуальность разработки программных средств для защиты изображений методами цифровой стеганографии объясняется интенсивным расширением спектра атак и их возможных последствий на мультимедийные системы, а также мультимедийный контент традиционных информационных систем. Необходимо отметить, что традиционные методы защиты электронных документов являются неэффективными для защиты мультимедийных систем.

В ходе работы был выполнен сравнительный анализ реализованных методов с использованием критерия отношения уровня сигнала к уровню шуму для различных популярных типов контейнеров, а также разработан новый алгоритм и автоматизированная система защиты мультимедийного контента.

Цифровые водяные знаки делятся на видимые и невидимые. Видимые водяные знаки довольно просто удалить или заменить, например, это можно сделать в графических редакторах, таких как Adobe Photoshop.

Задачу встраивания и выделения сообщений из другой информации выполняет стегосистема. Стегосистема состоит из следующих основных элементов, представленных на рисунке 1. Защита осуществляется путем встраивания водяного знака в изображение-контейнер.

К водяному знаку предъявляются следующие требования: водяной знак должен легко с вычислительной точки зрения извлекаться авторизованным пользователем, а также должен быть устойчивым либо неустойчивым к преднамеренным и случайным воздействиям, в зависимости от типа и целей защиты. Если водяной знак используется для подтверждения подлинности, то несанкционированное изменение контейнера должно приводить к разрушению водяного знака. Если же водяной знак содержит идентификационный код, логотип фирмы и т.п., то он должен сохраниться при максимальных искажениях контейнера, конечно, не приводящих к существенным искажениям исходного сигнала.

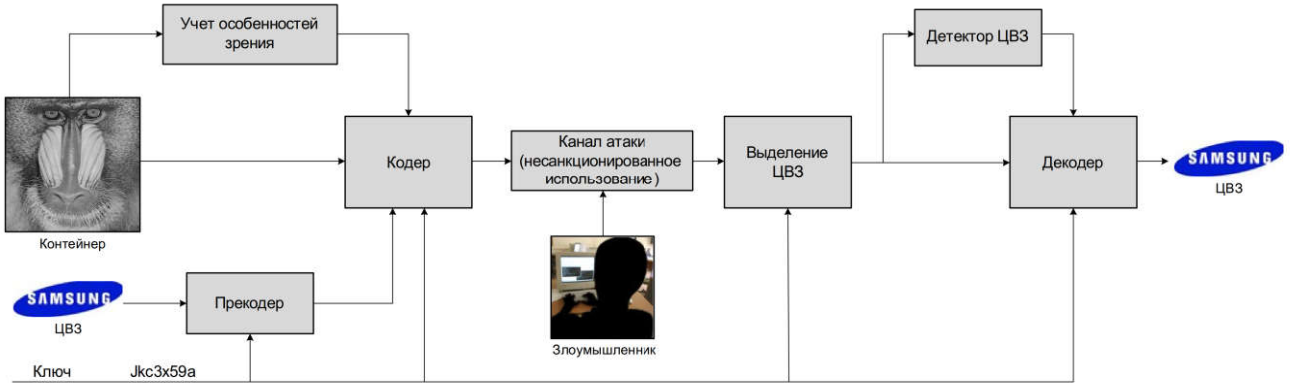

Рис. 1. Структурная схема разработанной стегосистемы цифровых водяных знаков

Например, у изображения могут быть отредактированы цветовые или яркостные характеристики. Необходимо отметить, что водяной знак должен быть робастным по отношению к аффинным преобразованиям изображения, то есть к его поворотам, масштабированию и т.п. При этом надо различать робастность самого водяного знака и способность детектора достоверно его обнаружить. Таким образом, при повороте изображения ЦВЗ не разрушится, а декодер может оказаться неспособным выделить его.

Изображения в современных системах электронного документооборота хранятся в заданном виде. Формат представления изображений основан на

некотором спектральном преобразовании, таком как дискретное косинусное преобразование, Фурье, Адамара, Пэли, Уолша, Трахтмана, Качмарджа, вейвлет-преобразование, и другие [3, 4]. В разработанной автоматизированной системе защиты используется быстрое преобразования Ле Галла [5].

Процедура встраивания предусматривает необходимость разбиения изображения на битовые плоскости, как показано на рисунке 2. Из рисунка 2 видно, что младшая битовая плоскость является шумом, человеческое зрение нечувствительно к изменениям в этой битовой плоскости.

В автоматизированной системе реализована возможность внедрения дополнительных водяных знаков. В случае, если в контейнере имеется метка о допустимости однократного использования, после осуществления использования контейнера, необходимо добавить пометку о запрете дальнейшего использования или водяной знак должен быть разрушен. Перезапись водяного знака в данном случае может вступать в противоречие с требованием робастности, поэтому одним из эффективных решений этой проблемы является внедрение дополнительного водяного знака, при котором внедренный ранее будет считаться недостоверным.

В ходе проведенной работы были проанализированы существующие алгоритмы и подходы к скрытию данных в изображениях, а также основные способы представления графической информации в системах электронного документооборота. Алгоритмы защиты изображений были разбиты на две основные группы: работающие в пространственной области и в частотной области. Были выделены классы изображений, т.к. любой стегоалгоритм имеет свою допустимую область, в которой может эффективно применяться. Кроме того, был проведен сравнительный анализ широкого спектра атак на стегосистему.

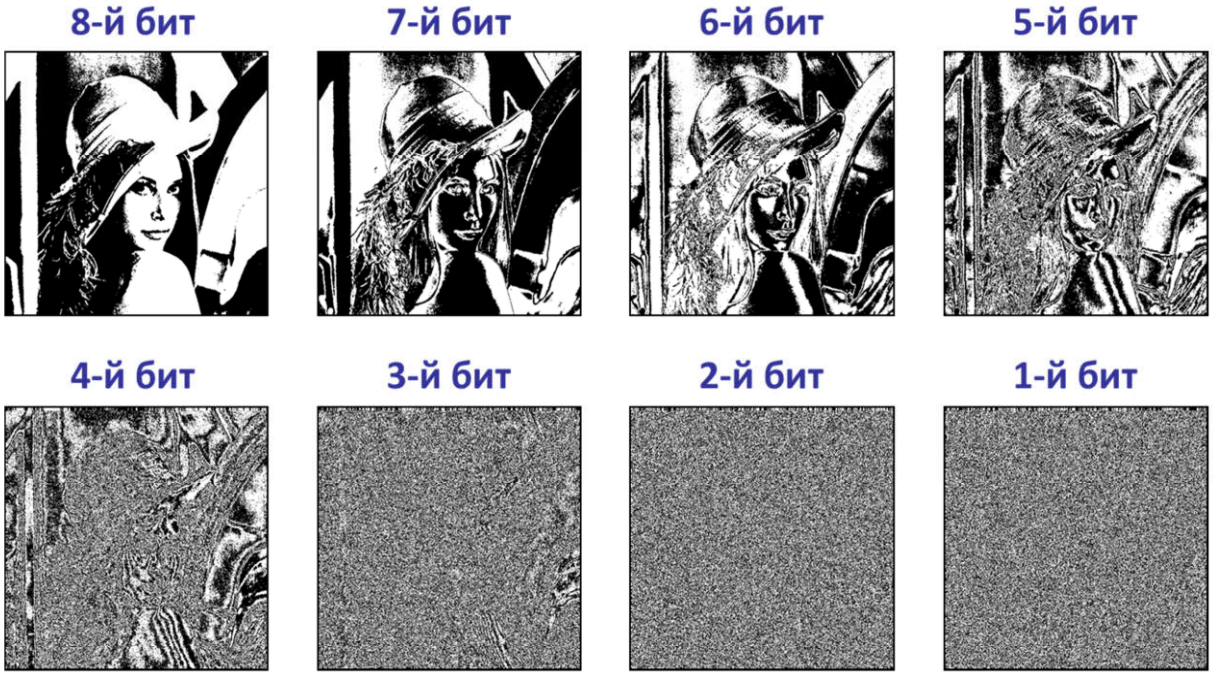

Рис. 2. Разбиение изображения на битовые плоскости

В ходе работы была разработана автоматизированная система защиты, соответствующая разработанной ранее классовой модели, а также реализован алгоритм стегокодирования на основе многоуровневого преобразования Ле Галла, и других вейвлет-преобразований [6, 7]. Система встраивания цифровых водяных знаков разрабатывается как приложение, основанное на каркасном подходе к построению информационных систем. Обобщенная структурная схема разработанной автоматизированной системы показана на рисунке 3.

Рис. 3. Структура разработанной автоматизированной системы защиты

В автоматизированной системе предусматривается чтение графических файлов различных современных форматов, что повысит объемы использования и степень внедрения автоматизированной системы защиты. Помимо основной функции программы, а именно – внедрение цифровых водяных знаков в изображения, предусмотрено сохранение в собственный формат кодирования, основанный на преобразовании Ле Галла.

Необходимо отметить, что алгоритмическая часть, отвечающая за операции с защитой изображений, полностью выделена в отдельные классы, не связанные с частью, осуществляющей взаимодействие с пользователем в процессе работы, что позволяет использовать классы, отвечающие за защиту изображений без переделок в других проектах.

Литература

1. Лавриченко, О.В. Управление инновационными системами промышленных предприятий и разработка модели их классификации / Лавриченко О.В. // Вестник Южно-Уральского государственного университета. Серия: Компьютерные технологии, управление, радиоэлектроника, 2014. Т. 14. № 4. С. 10.

2. Земцов А.Н., Болгов Н.В., Божко С.Н. Многокритериальный выбор оптимальной системы управления базы данных с помощью метода анализа иерархий // Инженерный вестник Дона, 2014, №2. URL: http://ivdon.ru/ru/magazine/archive/n2y2014/2360.

3. Земцов А.Н. Сравнительный анализ эффективности методов сжатия изображений на основе дискретного косинусного преобразования и фрактального кодирования // Прикладная информатика, 2011. № 5. С. 77-84.

4. Земцов А.Н. Сравнительный анализ эффективности методов сжатия изображений на основе дискретного косинусного преобразования и фрактального кодирования // Прикладная информатика, 2011. № 4. С. 90-104.

5. Земцов А.Н. Представление изображений с помощью преобразования Ле Галла // Вестник Томского государственного университета. Управление, вычислительная техника и информатика. 2018. № 43. С. 42-48.

6. Земцов А.Н., Аль-Макреби И.М. Об оценке вносимых искажений методом маркирования в низкочастотной области вейвлет-спектра изображения // Инженерный вестник Дона, 2015, №2-2(36). URL: http://ivdon.ru/ru/magazine/archive/n2p2y2015/2962.

7. Земцов А.Н., Аль-Макреби И.М. Исследование устойчивости цифровых водяных знаков-логотипов, внедряемых в статические изображения // Инженерный вестник Дона, 2015, №2-2(36). URL: http://ivdon.ru/ru/magazine/archive/n2p2y2015/2963.

С.А. Иливицкий[1], Л.С. Зеленко[1], П.В. Трешников[2]

РАЗРАБОТКА КОМПЛЕКСА ПРОГРАММ ДЛЯ ЛИЦЕНЗИРОВАНИЯ И РАСПРОСТРАНЕНИЯ ЛИЦЕНЗИЙ ПРОГРАММНОГО КОМПЛЕКСА «ТЕХНОДОК»

([1] Самарский университет, [2] ООО НВФ «Сенсоры. Модули. Системы»)

В настоящее время проблема защиты интеллектуальной собственности является актуальной для любой области творческой деятельности и не имеет гражданства. Большинство разработчиков программного обеспечения используют различные программные модули, контролирующие доступ пользователей с помощью ключей активации, серийных номеров и т. д. Однако такая защита легко подвержена взлому и не является достаточно надежной. В начале 1980 годов в качестве усовершенствования защиты программного обеспечения стали применяться электронные ключи. Они предоставили более надежный способ лицензирования программного обеспечения. Так же их использование позволило не привязываться к определенному аппаратному обеспечению, тем самым обеспечивая переносимость лицензионной информации с одного сервера на другой [1].