МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра теоретических основ компьютерной безопасности и криптографии

Повышение устойчивости встраиваемого водяного знака методом Коча к вредоносным воздействиям

АВТОРЕФЕРАТ

дипломной работы

студентки 6 курса 631 группы

специальности 10.05.01 Компьютерная безопасность

факультета компьютерных наук и информационных технологий

Стрельниковой Софии Юрьевны

Научный руководитель

доцент, к. п. н. _____ А. С. Гераськин

23.01.2020 г.

Заведующий кафедрой

д. ф.-м. н., доцент _____ М. Б. Абросимов

23.01.2020 г.

Саратов 2020

ВВЕДЕНИЕ

Существуют различные методы защиты авторских прав на мультимедийные файлы: цифровые подписи, шифрование, цифровые водяные знаки (ЦВЗ). Схожий с ЦВЗ принцип работы имеет цифровая подпись (ЦП) – реквизит электронного документа, полученный в результате криптографического преобразования информации с использованием закрытого ключа подписи и позволяющий проверить отсутствие искажения информации в электронном документе с момента формирования подписи (целостность), принадлежность подписи владельцу сертификата ключа подписи (авторство), а в случае успешной проверки подтвердить факт подписания электронного документа. ЦП обеспечивает защиту документа от искажения, подмены авторства, отказа от авторства [1].

Принцип работы ЦП заключается в следующем: для ее создания на основании данных документа вычисляется некоторая математическая хеш-функция, затем эта хеш-функция шифруется над закрытым ключом из личного сертификата пользователя, полученный результат является электронной подписью. Для расшифровки ЦП на основании данных документа снова вычисляется хеш-функция, затем берется цифровой сертификат пользователя, который подписал документ, и прикрепленная к документу ЦП, далее подпись расшифровывается на основе открытого ключа. Если хеш-функции совпадают, значит, подпись действительна [2].

Недостатком использования ЦП является то, что, если лицо, не являющееся автором документа, завладеет закрытым ключом, то оно с легкостью сможет подделывать чужую подпись. При использовании ЦВЗ такая проблема отсутствует. К тому же, если производить внедрение методом, предполагающим слепою схему извлечения ЦВЗ, можно сделать обнаружение ЦВЗ практически невозможным. Возможно также усиление защиты посредством внедрения нескольких различных водяных знаков в разные

области изображения, что делает посягательство на авторские права еще более затруднительным. Именно поэтому использование ЦВЗ является более предпочтительным способом защиты авторских прав [2][3].

Очень важно выбрать подходящий алгоритм встраивания ЦВЗ. Такой алгоритм должен быть устойчив к потенциальным атакам и возможным изменениям, которым может быть подвержено изображение в процессе работы с ним. Алгоритмы встраивания ЦВЗ отталкиваются от особенностей человеческого зрения и используют те же преобразования, что и алгоритмы сжатия. Поэтому, вложение производится в исходное, сжатое или подверженное сжатию в данный момент изображение.

Однако, использование ЦВЗ не гарантирует стопроцентной защиты, так как злоумышленник, желающий присвоить авторство себе, может попытаться избавиться от водяного знака законного собственника и даже встроить свой, ложный ЦВЗ. Сможет ли он это сделать, зависит от способа внедрения ЦВЗ и от вида самого водяного знака. Попытка злоумышленника нарушить или вовсе удалить цифровой водяной знак называется атакой. Существует целое множество атак, и в зависимости от вида ЦВЗ и способа и его встраивания он может быть устойчивым или неустойчивым к какой-либо из них. Атаки, использующие схожий принцип действия объединяются в классы [4][5].

При этом цифровой водяной знак должен в наименьшей мере искажать защищаемый контейнер. То есть ЦВЗ должны удовлетворять противоречивым требованиям незаметности и стойкости к основным операциям обработки сигналов [6].

Под стойкостью ЦВЗ понимается возможность корректного извлечения встроенной информации из носителя после того, как он был подвергнут некоторым искажениям. Иными словами, стойкость водяного знака характеризует простоту его удаления [7][8].

Целью данной дипломной работы является повышение устойчивости цифровых водяных знаков, встроенных методом Коча в изображения, к вредоносным воздействиям.

Задачи дипломной работы:

- рассмотрение классификации методов встраивания ЦВЗ в изображения с целью выбора метода для реализации;
- рассмотрение существующих классификаций ЦВЗ;
- рассмотрение классификации атак на системы цифровых водяных знаков;
- анализ стойкости метода Коча встраивания ЦВЗ в изображения;
- разработка и внесение в метод Коча модификаций, которые повлекут за собой повышение устойчивости цифровых водяных знаков, встроенных данным методом в изображения, к вредоносным воздействиям;
- анализ стойкости модифицированного метода Коча встраивания ЦВЗ в изображения к атакам с целью подтверждения или опровержения повышения стойкости алгоритма.

Дипломная работа состоит из введения, 4 разделов, заключения, списка использованных источников и 2 приложений. Общий объем работы – 70 страниц, из них 46 страниц – основное содержание, включая 32 рисунка и 2 таблицы, список использованных источников из 27 наименований.

КРАТКОЕ СОДЕРЖАНИЕ

В первом разделе дипломной работы, который называется «Классификация методов встраивания ЦВЗ в изображения», была рассмотрена классификация методов встраивания цифровых водяных знаков (ЦВЗ) в изображения. Далее на основании полученных данных был выбран наиболее актуальный класс методов встраивания, основанный на внедрении ЦВЗ в коэффициенты дискретного косинусного преобразования (ДКП). Среди методов встраивания, основанных на внедрении ЦВЗ в коэффициенты ДКП, для реализации был выбран метод Коча по критериям: тип ДКП, тип ЦВЗ, допустимого для внедрения, схема извлечения ЦВЗ, использование детектора или декодера при поиске/извлечении ЦВЗ из изображения.

Во втором разделе дипломной работы, который называется «Классификации цифровых водяных знаков», были рассмотрены классификации цифровых водяных знаков.

В третьем разделе дипломной работы, который называется «Классификация атак на системы цифровых водяных знаков», были рассмотрены две классификации атак на системы цифровых водяных знаков, из двух рассмотренных классификаций была выбрана вторая, как более полная.

В четвертом разделе дипломной работы, который называется «Модификация метода Коча», были получены данные об устойчивости ЦВЗ, встроенных методом Коча в изображения, к атакам из выбранной классификации. Было принято решение о внесении в метод Коча модификаций, которые должны повлечь за собой повышение устойчивости ЦВЗ к вредоносным воздействиям. После внесения соответствующих модификаций было проведено исследование, в ходе которого было установлено, что внесенные изменения действительно привели к повышению стойкости ЦВЗ, внедренных данным методом, к статистическим атакам. Показатели устойчивости к другим атакам не изменились.

ЗАКЛЮЧЕНИЕ

В ходе выполнения данной дипломной работы были рассмотрены: классификация методов внедрения цифровых водяных знаков в изображения, классификации цифровых водяных знаков, а также классификация возможных атак на системы цифровых водяных знаков.

На основании данных, полученных в ходе рассмотрения указанных классификаций для реализации был выбран метод внедрения цифровых водяных знаков в коэффициенты дискретного косинусного преобразования Коча. Далее был проведен анализ устойчивости данного метода к атакам из выбранной классификации. Данные для анализа были частично получены опытным путем, частично взяты из исследований других авторов. Было принято решение о внесении в реализованный алгоритм модификаций, которые должны повлечь за собой повышение устойчивости ЦВЗ к вредоносным воздействиям. После внесения соответствующих модификаций было проведено исследование, в ходе которого было установлено, что внесенные изменения действительно привели к повышению стойкости ЦВЗ, внедренных данным методом, к статистическим атакам. Показатели устойчивости к другим атакам не изменились.

В ходе анализа устойчивости ЦВЗ, встроенных в изображения модифицированным алгоритмом Коча к статистической атаке было установлено, что в 94% случаев из 100 на выборке из 100 изображений с различными параметрами наблюдалась устойчивость цифровых водяных знаков, что является хорошим показателем стойкости. Повышение устойчивости ЦВЗ к статистической атаке имеет место быть.

Все поставленные задачи были выполнены, цель достигнута.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Что такое электронная подпись – простым языком для новичков мира цифровой экономики [Электронный ресурс] // Единый портал электронной подписи [Электронный ресурс]] : [сайт]- . -URL: https://iecp.ru/articles/item/412631-ep-dlya-novichkov (дата обращения: 10.01.2020). - Загл. с экрана. - Яз. рус.

2 Как работает электронно-цифровая подпись [Электронный ресурс] // PKI Guru [Электронный ресурс] : [сайт]- . -URL: http://pkiguru.ru/forbeginers/2014/11/02/kak-rabotaet-elektronno-cifrovaya-podpis.html (дата обращения: 27.03.2018). - Загл. с экрана. - Яз. рус.

3 Цифровые водяные знаки – новые методы защиты информации [Электронный ресурс] // itWeek. Безопасность [Электронный ресурс] : [сайт]- . -URL: https://www.itweek.ru/security/article/detail.php?ID=105054 (дата обращения: 27.03.2018). - Загл. с экрана. - Яз. рус.

4 Cox, I.J. Digital Watermarking and Steganography [Электронный ресурс] / I.J. Cox, M. L. Miller, J. A. Bloom, J. Fridrich, T. Kalker. - 2-е изд. Morgan Kaufmann Publishers, 2008. - 587 с.- . -URL: http://bookre.org/reader?file=546994 (дата обращения: 27.09.2019). - Загл. с экрана. - Яз. англ.

5 Miller, M.L. A review of watermarking, principles and practices [Электронный ресурс] / M. L. Miller, I. J. Cox, M. G. Linnartz. T. Kalker. Digital Signal Processing in Multimedia Systems, 1999. - 32 с.- . -URL: http://bookre.org/reader?file=686344&pg=28 (дата обращения: 27.09.2019). - Загл. с экрана. - Яз. англ.

6 Аграновский, А. В. Стеганография, цифровые водяные знаки и стегоанализ [Электронный ресурс] / А. В. Аграновсикй, А. В. Балакин, В. Г. Грибунин, С. А. Сапожников, В. А. Федосеев // Монография [Электронный ресурс. - М.: Вузовская книга, 2009. - 217 с.- . -URL:

http://bookre.org/reader?file=1499464 (дата обращения: 27.09.2019). - Загл. с экрана. - Яз. рус. - Имеется печатный аналог.

7 Федосеев, В. А. Цифровые водяные знаки и стеганография [Электронный ресурс] / В. А. Федосеев // Учебное пособие с заданиями для практических и лабораторных работ [Электронный ресурс]. Самара: СГАУ, 2015. - 128 с.- . -URL: https://ru.b-ok.cc/book/3555680/2d863f (дата обращения: 27.09.2019). - Загл. с экрана. - Яз. рус.

8 Barni, M. Watermarking Systems Engineering [Электронный ресурс] / M. Barni, F. Bartolini. New York: Basel, 2004. - 485 с.- . -URL: http://bookre.org/reader?file=490553&pg=1 (дата обращения: 27.09.2019). - Загл. с экрана. - Яз. англ.

9 Стеганография и путешествия. Замена наименее значащего бита или LSB // Блог о компьютерной стеганографии, путешествиях по России и миру, а также палеонтологии и вымерших существах [Электронный ресурс] - . -URL: http://www.nestego.ru/2012/07/lsb.html (дата обращения: 27.03.2018). - Загл. с экрана. - Яз. рус.

10 Стеганографический метод Куттера-Джордана-Боссена [Электронный ресурс] // Хабр [Электронный ресурс] - . -URL: https://habr.com/ru/post/115287/ (дата обращения: 10.01.2020). - Загл. с экрана. - Яз. рус.

11 Национальная библиотека имени Н. Э. Баумана. Bauman National Library. Сокрытие данных методами стеганографии [Электронный ресурс] : [сайт]- . -URL: http://ru.bmstu.wiki/Сокрытие_данных_методами_стеганографии (дата обращения: 03.04.2018). - Загл. с экрана. - Яз. рус.

12 Белобокова, Ю. С. Модели и алгоритмы защитной маркировки для обеспечения аутентичности и целостности растровых изображений: диссертация на соискание ученой степени кандидата технических наук [Электронный ресурс] / Ю. С. Белобокова. - Москва, 2014. - 112 с.- . -URL: https://elibrary.ru/item.asp?id=30410171 (дата обращения: 27.11.2019). - Загл. с экрана. - Яз. рус.

13 Земцов, А.Н. Робастный метод цифровой стеганографии на основе дискретного косинусного преобразования [Электронный ресурс] / А . Н. Земцов // Известия Волгоградского государственного технического университета. Общие и комплексные проблемы технических и прикладных наук и отраслей народного хозяйства [Электронный ресурс]. - 2011. - Т. 11, № 12. - С. 141 – 144. - . -URL: https://vivliophica.com/articles/apsciences/441379 (дата обращения: 27.11.2019). - Загл. с экрана. - Яз. рус.

14 Гонсалес, Р. Цифровая обработка изображений [Электронный ресурс] / Р. Гонсалес, Р. Вудс ; перевод с английского под редакцией П. А. Чочиа. - М.: Техносфера. - 2005. - 1073 с.- . -URL: https://ru.b-ok.cc/book/2404835/ad9df5 (дата обращения: 29.09.2019). - Загл. с экрана. - Яз. рус.

15 Методы компьютерной обработки изображений [Электронный ресурс] / под ред. В.А. Сойфера. - 2-е изд. - М.: Физматлит, 2003. - 778 с.- . -URL: http://bookre.org/reader?file=474663&pg=1 (дата обращения: 29.09.2019). - Загл. с экрана. - Яз. рус.

16 Амплитудная модуляция на пальцах [Электронный ресурс] // Habr [Электронный ресурс]- . -URL: https://habr.com/ru/post/416181/ (дата обращения: 30.09.2019). - Загл. с экрана. - Яз. рус.

17 Шумоподавление посредством усреднения изображений [Электронный ресурс] // Cambridge in colour. A learning community for photographers [Электронный ресурс]- . -URL: https://www.cambridgeincolour.com/ru/tutorials-ru/image-averaging-noise.htm (дата обращения: 01.10.2019). - Загл. с экрана. - Яз. рус.

18 Атаки на системы цифровых водяных знаков [Электронный ресурс] // indbooks [Электронный ресурс]- . -URL: http://indbooks.in/mirror6.ru/?p=277987 (дата обращения: 01.10.2019). - Загл. с экрана. - Яз. рус.

19 Аффинное преобразование и его матричное представление [Электронный ресурс] // Компьютерная графика. Теория, алгоритмы, примеры на C++ и OpenGL [Электронный ресурс]- . -URL:

https://compgraphics.info/2D/affine_transform.php (дата обращения: 03.10.2019). - Загл. с экрана. - Яз. рус.

20 Грибунин, В. Г. Статистические атаки на стегосистемы с изображениями-контейнерами [Электронный ресурс] / В. Г. Грибунин // ВикиЧтение. Цифровая стеганография [Электронный ресурс]- . -URL: https://tech.wikireading.ru/13267 (дата обращения: 05.10.2019). - Загл. с экрана. - Яз. рус.

21 Шапиро, Л. А. Статистическая оценка параметров распределений [Электронный ресурс] / Л. А. Шапиро // Кафедра медицинской и биологической физики. Лекция №2 [Электронный ресурс]- . -URL: https://ppt-online.org/204038 (дата обращения: 05.10.2019). - Загл. с экрана. - Яз. рус.

22 Критерий согласия Пирсона χ^2 (Хи-квадрат). Проверка гипотез [Электронный ресурс]- . -URL: https://statanaliz.info/statistica/proverka-gipotez/kriterij-soglasiya-pirsona-khi-kvadrat/ (дата обращения: 25.11.2019). - Загл. с экрана. - Яз. рус.

23 Дрюченко, М. А. Алгоритмы выявления стеганографического скрытия информации в JPEG-файлах [Электронный ресурс] / М. А. Дрюченко // Вестник ВГУ. Серия Системный анализ и информационные технологии. -2007. №3. - С. 21 – 30.

24 Грачева, Ю. А. Применение цифровых водяных знаков для защиты цифровых фотографий [Электронный ресурс] / Ю. А. Грачева. - Московский государственный университет печати, кафедра «Медиасистемы и технологии». - С. 52 – 57.- . -URL: https://elibrary.ru/item.asp?id=18258960 (дата обращения: 03.10.2019). - Загл. с экрана. - Яз. рус.

25 Демидчук, А. И, Чернявский Ю. А. Алгоритм поиска в изображениях скрытых данных, встроенных методом Коха-Жао [Электронный ресурс] / А. И. Демидчук, Ю. А. Чернявский // Белорусский государственный университет информатики и радиоэлектроники. -2011. - С. 39 - 46.- . -

URL: https://inf.grid.by/jour/article/viewFile/307/283 (дата обращения: 10.01.2020). - Загл. с экрана. - Яз. рус.

26 Гераськин, А. С., Стрельникова, С. Ю, Завенягин, М. П. Исследование возможности улучшения реализации алгоритма метода Коча для встраивания цифровых водяных знаков в изображения [Электронный ресурс] / А. С. Гераськин, С. Ю. Стрельникова, М. П. Завенягин // Безопасность информационных технологий. - 2018. - Т. 25, №4. - С. 86 – 94.- . - URL: https://bit.mephi.ru/index.php/bit/article/view/1166/1126 (дата обращения: 10.01.2020). - Загл. с экрана. - Яз. рус.

27 Встраивание ЦВЗ в изображения методом Коча (Koch) : отчет о НИР (заключ.) [Электронный ресурс] / Саратовский национальный исследовательский государственный университет имени Н. Г. Чернышевского ; рук. М. Б. Абросимов ; исполн.: С. Ю. Стрельникова. - Саратов, 2019. - 37 с.