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

Реализация программного модуля внедрения ЦВЗ пространственным методом

АВТОРЕФЕРАТ
дипломной работы

студента 6 курса 631 группы
специальности 10.05.01 Компьютерная безопасность
факультета компьютерных наук и информационных технологий
Ступина Артема Сергеевича

Научный руководитель
доцент, к.п.н. _____ А. С. Гераськин
22.01.2024 г.

Заведующий кафедрой
д. ф.-м. н., доцент _____ М. Б. Абросимов
22.01.2024 г.

Саратов 2024

ВВЕДЕНИЕ

В современном мире все больше различных аспектов жизнедеятельности общества переходят к цифровым технологиям. От создания сложнейших вычислительных машин, контролирующих запуск космических кораблей, и нейросетей, способными управлять всем цифровым бытом человека, до оформления различных электронных договорах, которые также не обходятся без все большего и большего вмешательства цифровых технологий.

Для того чтобы можно было безопасно обмениваться конфиденциальными данными по сети, их необходимо защитить. Одним из таких средств защиты является нанесение цифровых водяных знаков на документ. Эта технология передачи важной информации в системах документации путем сокрытия сообщений в цифровых сигналах. С помощью цифровых водяных знаков можно скрывать системную информацию в документах, организовывать защиту документа, в том числе снимков и других изображений. При обладании ключом, необходимым для извлечения цифрового водяного знака, можно легко удостовериться в подлинности полученного сообщения или идентифицировать авторские права на какой-либо цифровой документ [6].

В свою очередь факт внедрения ЦВЗ не гарантирует полной реализации той цели, для которой он внедрялся. Например, в случае опровержения авторских прав на изображение, оно может подвергнутся атаке, в результате которой пострадает и цифровой водяной знак нанесенный на данное изображение. В таком случае для этого злоумышленнику в первую очередь важно сохранить без повреждений исходное изображение и по максимуму уничтожить ЦВЗ.

Все вышеизложенное обусловливает актуальность выбранной темы исследования.

Целью данного исследования является реализация метода внедрения цифровых водяных знаков в графические изображения пространственным методом и оценка стойкости к атакам.

Задачи исследования:

1. Провести анализ литературных источников по данной проблеме.

2. Доработать пространственный метод внедрения цифровых водяных знаков для устойчивости от некоторых видов атак.

3. Провести анализ полученных результатов и сделать вывод.

Дипломная работа состоит из введения, 2 глав, заключения, списка использованных источников и 2 приложений. Общий объем работы – 58 страниц, из них 40 страниц – основное содержание, включая 33 рисунка и 2 таблицы, список использованных источников из 20 наименований.

КРАТКОЕ СОДЕРЖАНИЕ

Глава 1 Методы встраивания цифровых водяных знаков в изображения

В данной главе описываются методы и алгоритмы встраивания, а также рассматриваются их плюсы и минусы при реализациях различных видов атак на ЦВЗ.

1.1 Методы встраивания цифровых водяных знаков

В настоящее время существует множество способов встраивания ЦВЗ, которые можно разделить на три класса: пространственные, частотные и основанные на моментах.

Пространственные алгоритмы внедряют ЦВЗ в исходное изображение посредством манипуляций яркостью или цветовыми составляющими. Их преимуществом является то, что нет необходимости выполнять преобразования изображений. Недостатком таких алгоритмов является слабая устойчивость к различным операциям обработки изображения.

Частотные алгоритмы, основанные на преобразованиях изображения, реализуются сложнее, так как перед внедрением ЦВЗ необходимо «перераспределить энергию» контейнера, чтобы встроить сообщение в специальные спектральные области. За счет подобной декомпозиции изображения ЦВЗ становится робастным к внешним атакам.

Методы, основанные на моментах изображений, применяются для защиты ЦВЗ от геометрических преобразований контейнера. Однако они имеют узкую направленность, а их основным недостатком является низкий уровень безопасности от других видов атак.

1.2 Алгоритмы внедрения цифровых водяных знаков

Рассмотрим наиболее часто встречающиеся в литературе алгоритмы внедрения цифровых водяных знаков в изображение.

Алгоритмы на основе линейного встраивания данных. В аддитивных методах внедрения ЦВЗ представляет собой последовательность чисел ω_i длины N, которая внедряется в выбранное подмножество отсчетов исходного изображения f. Основное и наиболее часто используемое выражение для встраивания информации в этом случае

$$f'(m,n) = f(m,n)(1 + \alpha\omega_i), \quad (1)$$

где α - весовой коэффициент, а f' – модифицированный пиксел изображения.

Для увеличения робастности внедрения во многих алгоритмах применяются широкополосные сигналы.

Основным недостатком этого метода является то, что само изображение в этом случае рассматривается, как шумовой сигнал.

Алгоритмы на основе слияния ЦВЗ и контейнера. Если вместо последовательности псевдослучайных чисел в изображение встраивается другое изображение, например, логотип фирмы, то соответствующие алгоритмы внедрения называются алгоритмами слияния. Размер внедряемого сообщения намного меньше размера исходного изображения. Перед встраиванием оно может быть зашифровано или преобразовано каким-нибудь иным образом.

У таких алгоритмов есть два преимущества. Во-первых, можно допустить некоторое искажение скрытого сообщения, так как человек все равно сможет распознать его. Во-вторых, наличие внедренного логотипа является более убедительным доказательством прав собственности, чем наличие некоторого псевдослучайного числа.

Алгоритмы встраивания ЦВЗ с использованием скалярного квантования. В данном алгоритме к цветному изображению первоначально применяется пятиуровневое целочисленное вейвлет-преобразование. ЦВЗ представляет собой последовательность ± 1. Модификации подвергаются только высокочастотные коэффициенты голубой компоненты, так как

человеческий глаз наименее чувствителен к искажениям в этой области спектра.

Алгоритмы встраивания ЦВЗ с использованием векторного квантования. В предыдущем разделе рассматривался случай, когда на вход квантователя подавались скалярные значения, и каждое кодовое слово квантователя представляло собой единичный отсчет выхода источника. Стратегия квантования, которая предусматривает работу с последовательностями или блоками отсчетов называется векторным квантованием. Проблема в этом случае состоит в генерации множества последовательностей, называемой кодовой книгой.

1.3 Атаки на графическое изображение

Наибольший интерес представляют внешние воздействия на стегоконтейнер, так называемые атаки. Атаки на водяные знаки нацелены на полное удаление или предотвращение использования водяных знаков при сохранении первоначального качества изображения. Важным аспектом любой схемы водяных знаков является ее устойчивость к атакам. Понятие устойчивости интуитивно понятно: водяной знак является надежным, если его нельзя нарушить и не сделать при этом бесполезными атакованные данные.

Пассивная атака предполагает определение наличие скрытого цифрового водяного знака «на глаз». Она является наиболее безопасной, так как не несет в себе никакой угрозы контейнеру и его содержимому.

Активные атаки делятся на две группы воздействия: направленные на извлечение и на разрушение цифрового водяного знака. В случае, когда целью злоумышленника является получение информации, ему не предназначенной, остановить его можно путем шифрования данных (использование криптографической защиты) или использования модифицированных методов нанесения ЦВЗ, отличающихся от общеизвестных [13].

Активные атаки водяных знаков могут классифицироваться как атаки удаления, геометрические атаки, криптографические атаки и протокольные атаки.

Вывод по главе 1

По результатам теоретического исследования можем сделать вывод, что пространственные методы внедрения ЦВЗ обладают преимуществом в отсутствии необходимости выполнять какие-либо преобразования исходного изображения. В случае пассивных атак на контейнер с таким методом встраивания цифрового водяного знака, злоумышленнику не удастся определить наличие ЦВЗ в исходном изображении, особенно если выбрать хороший алгоритм встраивания ЦВЗ. Однако, в случае реализации злоумышленником активных атак, данный метод не обладает высоким коэффициентом устойчивости. В практической части нашего исследования доработаем данным метод встраивания и изъятия ЦВЗ для противостояния атакам путем обрезки и зеркалирования изображения. В качестве алгоритма для реализации пространственного метода встраивания цифрового водяного знака был выбран алгоритм на основе слияния ЦВЗ и контейнера при помощи вейвлет-преобразований. Для проверки робастности были реализованы самые частые атаки, применяемые к данному методу.

Глава 2 Программная реализация

В результате исследования проведенного в рамках дипломной работы был программно модифицирован модуль встраивания ЦВЗ пространственным методом. Данная программа написана на языке Python.

2.1 Описание модуля встраивания ЦВЗ и программы по реализации атак

Данная программа позволяет встроить цифровой водяной знак в графическое изображение. В качестве контейнера на выбор предлагается одно из нескольких изображений, а также можно выбрать один из трех ЦВЗ для встраивания. Также программа позволяет изъять ЦВЗ из изображения.

После выбора исходного изображения и изображение, которое будет являться цифровым водяным знаком, встроим его в исходных контейнер. Далее прежде чем изъять ЦВЗ из изображения подвергнем наш контейнер реализованными атаками на ЦВЗ. В данной работе реализованы атаки путем обрезки и зеркалирования изображения, пережатие другим форматом и шумовая атака. Будем последовательно реализовать каждую из атак и производить изъятие цифрового водяного знака. В случае использования пространственного метода встраивания ЦВЗ без каких-либо доработок все атаки, кроме шумовой, приводят к полному уничтожению ЦВЗ. Шумовая атака уничтожает цифровой водяной на, примерно, 40%.

В случае использования модифицированного метода внедрения, удалось добиться полной защиты от атаки зеркалирования и обрезки изображения путем встраивания в выбранную значимую область изображения.

Вывод по главе 2

В результате тестирования программы выявлено, что при помощи доработки алгоритма внедрения и изъятия ЦВЗ удалось добиться защиты от геометрических атак, а именно от обрезки и зеркалирования изображения. Реализации шумовой атаки без видимых изменений исходного контейнера не

уничтожает полностью встроенный цифровой водяной знак. ЦВЗ сохраняется на более чем 60%, в результате чего не теряется главное свойство ЦВЗ – подтверждение авторского права. Для защиты от атаки сжатием лучше выбрать частотный метод встраивания ЦВЗ, так как без перераспределения энергии контейнера на низкочастотные и высокочастотные области здесь не обойтись.

ЗАКЛЮЧЕНИЕ

В ходе данного исследования мы познакомились с понятием цифрового водяного знака, рассмотрели механизмы внедрения цифровых водяных знаков, а также рассмотрели возможные варианты атак на ЦВЗ.

Применение невидимых цифровых водяных знаков позволяет сократить потери от угроз хищения, в том числе незаконного копирования, использования изображений и является перспективным направлением в обеспечении защиты авторских прав, так как ЦВЗ обладает сравнительно невысокой стоимостью, в отличие от других технических методов, невидим для злоумышленника и подходит при регистрации цифровых изображений.

Существует несколько различных способов внедрения ЦВЗ. Каждый из которых обладает своими уникальными свойствами. В данной работы мы изучили и более широко осветили алгоритмы на основе слияния ЦВЗ и контейнера. Также рассмотрели классификацию атак на цифровые водяные знаки, внедренные в графическое изображение. Написали собственную программу по реализации данных атак.

Исходя из полученных результатов можно сделать вывод, что наша программа по внедрению и извлечению ЦВЗ не дает защиты от активных атак. При воздействии на стегоконтейнер любой из геометрических атак, сжатием изображения в другой формат или воспроизведение шумовой атаки ЦВЗ разрушается. При некоторых атаках реализованный механизм изъятия цифрового водяного знака из изображения в принципе не дает правильного результата, что является полным уничтожением ЦВЗ в изображении.

Для повышения робастности была произведена доработка данного алгоритма внедрения и извлечения ЦВЗ. В частности, для защиты от атаки путем обрезки изображения мы можем задать по координатам необходимую область для встраивания ЦВЗ, которая не будет задета обрезкой, в результате чего цифровой водяной знак, встроенный в данную область, извлекается без каких-либо потерь. Выбор необходимой области мы можем сделать на

основании исходного изображения путем анализа, какая область данного изображения является наиболее ценности для сохранения. Для защиты от зеркальной атаки доработанный алгоритм производит изъятие из всевозможных вариантов расположения исходного изображения. В случае нахождения совпадения выдает правильный результат в виде встроенного ЦВЗ.

Универсального способа защита от атак на графические изображения со встроенными цифровыми водяными знаками не существует. Различные методы и алгоритмы встраивания могут иметь свои плюсы и минусы при защите от разных видов атак. На примере данной работы мы убедились, что, используя достаточно простой в реализации метод встраивания ЦВЗ, можно без использования дополнительных преобразований контейнера добиться защиты от нескольких различных атак путем модификации и улучшения исходного алгоритма встраивания и изъятия цифрового водяного знака.