МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»
(СГУ)

Кафедра теоретических основ компьютерной безопасности и криптографии

Практические применения стеганографии

АВТОРЕФЕРАТ
дипломной работы

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

Научный руководитель
доцент _____ 18.01.2019 г. И. Ю. Юрин

Заведующий кафедрой
д. ф.-м. н., доцент _____ 18.01.2019 г. М. Б. Абросимов

Саратов 2019

ВВЕДЕНИЕ

Стеганография, как наука о сокрытии информации, в современном мире получила довольно большую долю внимания в контексте защиты передаваемой информации от несанкционированного обнаружения и ознакомления. Причем цифровая стеганография, начиная с описания Симмонсом задачи заключенных, получила широкое развитие. Были разработаны всевозможные алгоритмы и протоколы, позволяющие скрытие всевозможной информации в практически всех возможных стеганографических контейнерах с учетом необходимых требований, описаны протоколы безопасного обмена данными при различных атаках и изучены возможные слабости.

Однако, несмотря на это, непосредственное ее применение по прежнему ограничивается, в основном, скрытием непосредственно передачи некоторой секретной информации по открытому каналу связи. Причем, даже в контексте одной этой задачи с примерно одинаковыми требованиями, реализации различных методов зачастую несовместимы между собой, не позволяя простого переключения между ними при необходимости. И тем более, когда с помощью стеганографии решаются альтернативные задачи, например, аутентификации, имеющие решения имеют ряд недостатков, возникающих из-за их сложности и уникальности подходов к их реализации.

Целями данной работы являются:

Описание теоретической стеганографической модели, позволяющей унифицировать реализации произвольных стеганографических систем и алгоритмов, демонстрация ее универсальности и защищенности в классической задаче скрытой передачи данных, а так же реализация для демонстрации возможностей и использования;

Обзор применения стеганографии в задаче аутентификации пользователей, анализ существующих решений, а так же разработка собственного метода на основе разработанной модели и необходимого инструментария для его использования;

Рассмотрение возможностей применения стеганографии в задаче сжатия данных, разработка необходимой теории и алгоритмов, описания требований и свойств создание и демонстрация на их основе программного продукта, а так же анализ эффективности его применения.

Дипломная работа состоит из введения, четырех разделов, заключения, списка использованных источников и семи приложений. Общий объем работы — 108 страниц, из них 62 страницы — основное содержание, включая 23 рисунка и одну таблицу, список использованных источников из 14 наименований.

КРАТКОЕ СОДЕРЖАНИЕ

Первый раздел, «**Основные теоретические сведения и определения**», содержит минимальное подмножество общей терминологии, использующейся в работе и состоящей из набора определений и понятий, связанных со стеганографией.

Второй раздел, «**Разработка модели универсальной стеганографической системы**», посвящен описанию теоретической модели от более общих понятий к более частным, доказательству ее универсальности и защищенности как стеганографической системы, а так же описанию ее основных свойств. Он состоит из пяти подразделов.

В первом подразделе 2.1 «**Представление стеганографического контейнера**» описывается, каким образом в разрабатываемой модели будут представляться произвольные стеганографические контейнеры.

В следующем за ним подразделе 2.2, «**Механизме встраивания и извлечения данных**», представляется модель абстрактного стеганографического устройства, описание его структуры и составляющих, а так же описывается механизм работы с помощью определения понятия инструкций, их типов и схем работы. Вместе с инструкциями вводится понятие стеганографической программы, рассматриваются их типы и зависимость от набора инструкций. В заключение подраздела приводится схема стеганографической системы на основе абстрактного стеганографического устройства.

Следующий подраздел, 2.3, «**Универсальность стеганографической системы на основе абстрактного стеганографического устройства**», предоставляет доказательство, как и указано в названии, универсальности такой стеганографической системы. Для этого вводятся понятия универсальности и оракула, после чего доказательство проводится проводится по построению с помощью двух алгоритмов — алгоритма построения произвольного оракула и алгоритма создании им программы для произвольных входных данных и сделаны соответствующие выводы.

В подразделе 2.4, «**Защищенность стеганографической системы на основе абстрактного стеганографического устройства**», вводится понятие защищенности стеганографической системы и рассматривается с точки зрения защищенности оракулов и непосредственно программ стеганографического устройства. Защищенность программ рассматривается с точки зрения сложности обнаружения и несанкционированного извлечения встроенной в стеганографический контейнер информации, делается вывод о нерациональности проведения атак в общем случае и предлагается подход, делающий их (атаки) нерациональными в каждом частном случае. Защищенность оракулов рассматривается с точки зрения сложности предсказания будущих программ, строящихся им, по известным предыдущим значениям.

Подраздел 2.5 «**Программная реализация стеганографической системы на основе абстрактного стеганографического устройства**» представляет описание реализации библиотеки для создания общего интерфейса и упрощения реализаций абстрактных стеганографических устройств на языке программирования C стандарта C99. В нем же приводится пример реализации такой системы с использованием разработанной библиотеки на основе метода LSB в стеганографических контейнерах, представленных изображениями в формате PNG, и пользовательского приложения для работы с ней. Для реализации приводится пример использования и описывается механизм работы.

Таким образом, во втором разделе приведена рабочая модель универсальной стеганографической системы с ее подробным описанием, была доказана ее универсальность и защищенность, для ее практического применения была разработана универсальная кросс-платформенная библиотека, а для демонстрации ее работы стеганографическая система на основе и интерпретатор для взаимодействия с пользователем.

Третий раздел, «**Стеганографическая аутентификация пользователей**», посвящен рассмотрению задачи аутентификации пользователей с точки зрения использования стеганографических методов и скрытия ее процесса.

Подраздел 3.1, «**Решаемые задачи**» описывает задачи, которые можно решить с использованием стеганографической аутентификации, то есть возможности ее практического применения. При этом формулируется общий вид требований к таким задачам, каждое из которых рассматривается отдельно, с приведением примеров, возникающих в реальном мире.

Подраздел 3.2, «**Существующие методы и решения**», содержит анализ существующих решений рассмотренных задач с использованием методов стеганографии, таких как цифровые водяные знаки, системы на основе общего секрета, схемы разделения секрета, методы асимметрической стеганографии, а так же сокрытие не стеганографических протоколов. Для каждого решения были описаны его применения и недостатки в контексте рассматриваемой задаче.

Следующий подраздел, 3.3, «**Об асимметричности программ стеганографического устройства**», посвящен рассмотрению стеганографических программ с точки зрения различия оных для встраивания и извлечения информации. Для найденных особенностей были сформулированы и продемонстрированы две операции, позволяющие реализацию асимметричности в стеганографической системе на основе абстрактного стеганографического устройства, рассмотрены их особенности.

В подразделах 3.4 и 3.5, «**Примитивный протокол стеганографической аутентификации**» и «**Протокол аутентификации с использованием абстрактного стеганографического устройства**» соответственно, приводятся простой протокол стеганографической аутентификации на основе некоторой симметрической системы, после чего, с использованием обнаруженных особенностей программ абстрактного стеганографического устройства, был перезаписан в форме двухэтапного протокола асимметрической аутентификации пользователя с использованием стеганографической системы на его основе.

Раздел 3.6, «**Создание оракула для выработки аутентифицирующих программ**», представляет описание разработанной программы для проведения первого этапа разработанного протокола — этапа выработки аутентификационной информации — на языке программирования C стандарта

C99, демонстрируется процесс работы с ней, а так же делается замечание о существовании всего необходимого для проведения данного протокола инструментария за счет разработанных в работе средств.

Подраздел 3.7, «**Использование аппаратного токена для аутентификации пользователя с использованием разработанной модели**», вводит понятие токена аутентификации, после чего, на примере устройства Orange Pi i96, демонстрируется его использования в разработанном протоколе. В нем приводится описание разработанных средств для использования токена по описанному назначению, а так же пользовательского приложения для взаимодействия с ним, как и протокола, по которому данное взаимодействие происходит.

Подводя итог, третий раздел приводит описание задач, теорию для их решения, а так же разработанное непосредственно в данной работе решение, выраженное протоколом аутентификации с использованием особенностей стеганографической системы на основе абстрактного стеганографического устройства, а так же создан необходимый для его защищенного применения набор программных и аппаратных средств.

Четвертый раздел, «**Сжатие данных с использованием методов стеганографии**», посвящен описанию задачи стеганографического сжатия данных, созданию теоретического и практического аппарата для его (сжатия) фактического проведения, а так же описания возможностей применения подобных техник в современном мире.

Подразделы 4.1 — 4.2, «**Механизм упаковки и распаковки данных**» и «**Использование стеганографического алгоритма сжатия данных**», формулируют математически понятие стеганографического алгоритма сжатия данных, стеганографического архива, а так же описывают общий вид алгоритмов его упаковки и распаковки.

Подраздел 4.3, «**Применения стеганографического сжатия данных**», классифицирует и кратко описывает возможности применения подобного сжатия

данных, приводя в качестве примера произвольную клиент-серверную модель и схему использования оного в ней.

Следующий подраздел, 4.4, «**Возможности и требования при реализации сжатия данных с помощью стеганографии**», описывает, какие ограничения накладываются на стеганографические алгоритмы при выборе кандидатов на реализацию стеганографического алгоритма сжатия данных, приводя примеры как удачных, так и менее удачных кандидатов.

В подразделе 4.5, «**Выбор алгоритма стеганографии для практической реализации**», проводится анализ алгоритма стеганографии F5 с точки зрения описанных требований и эффективности его применения в задаче сжатия данных. При этом приводится описание механики его работы, связанных с ней особенностей и формального описания оригинального алгоритма скрытия информации с его использованием.

Подраздел 4.6, «**Стеганографический алгоритм сжатия на основе алгоритма стеганографии F5**», описывает необходимые модификации и мотивацию для них для превращения алгоритма скрытия данных в алгоритм сжатия данных. Описывается формат реализации стеганографического архива, его представления на файловой системе, особенности при использовании алгоритма F5, а так же формально описываются алгоритмы создания архива и восстановления из него информации.

В подразделе 4.7, «**Разработка библиотеки для реализации стеганографических алгоритмов сжатия**», представляется единый интерфейс для алгоритмов стеганографического сжатия данных и библиотека-шаблон для создания его реализаций. Для библиотеки также приводится описание необходимых для создания такой реализаций шагов.

Подраздел 4.8, «**Программная реализация стеганографического алгоритма сжатия на основе алгоритма стеганографии F5**», описывает создание кросс-платформенной утилиты (программы) для проведения стеганографического сжатия пользователями. Разработанная утилита демонстрируется с точки зрения метода работы и интерфейса взаимодействия с

пользователем, после чего используется для проведения тестирования и демонстрации эффективности выбранного подхода и его реализации. Из полученных в ходе тестирования результатах делаются выводы о возможностях и особенностях применения алгоритма F5 в задаче стеганографического сжатия данных.

То есть, в четвертом разделе подробно рассматривается применение стеганографического сжатия данных, формулируется вся необходимая теория для реализации подобных алгоритмов. Для практической демонстрации возможностей использования анализируются некоторые алгоритмы стеганографии, после чего описывается в качестве подходящего кандидата с указанием причин алгоритм F5 и реализация соответствующего алгоритма стеганографического сжатия данных, а так же программного обеспечения для его проведения. С использование разработанного проводится демонстрация и анализ эффективности метода стеганографического сжатия F5 в условиях, приближенных к реальным сценариям использования, при этом делаются выводы как о его преимуществах, так и недостатках.

ЗАКЛЮЧЕНИЕ

Методы стеганографии в настоящее время являются очень недооцененными и, если применяются, то для решения очень узкого круга задач, а сами решения зачастую являются неудобными с точки зрения их реализации и универсальности предоставляемых интерфейсов.

В данной работе была разработана универсальная модель, позволяющая реализовывать произвольные стеганографические алгоритмы и системы с помощью единого интерфейса, доказана ее универсальность, показана защищенность в задаче скрытого обмена информацией. Для демонстрации работы и будущего использования модели была разработана программная реализация мульти-платформенной библиотеки на языке программирования C, с ее использованием разработана стеганографическая система и продемонстрирована корректность ее работы.

Помимо этого, было подробно рассмотрено применение стеганографии в задаче аутентификации пользователей, а так же существующие ее решения, показаны их недостатки. С учетом сказанного, на основе разработанной в этой же работе и упомянутой выше модели был разработан протокол асимметричной аутентификации пользователей и продемонстрированы его потенциальные применения, а так же достоинства относительно других решений.

И если эти результаты работы описывали в основном привычные применения стеганографии и решения для них, то в завершение работы было рассмотрено применение стеганографии в задаче сжатия данных. Разработанная теория и алгоритмы были реализованы в качестве универсальной библиотеки для реализации программ сжатия с использованием алгоритмов стеганографии и утилите на ее основе для создания стеганографических архивов из библиотек JPEG-файлов с помощью алгоритма стеганографии F5. После чего с помощью разработанной утилиты была продемонстрирована крайняя эффективность сжатия данных подобными средствами, особенно, на фоне классических средств.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Руководящий документ Гостехкомиссии России. Защита от несанкционированного доступа к информации. Термины и определения. М. : ГТК РФ, 1992.

2 Frank, Y. S. Digital watermarking and steganography: fundamentals and techniques / Frank Y. Shih. CRC Press, 2007.

3 Tirkel, A. Z. Electronic Water Mark / A. Z. Tirkel, G. A. Rankin, R. M. Van Schyndel, W. J. Ho, N. R. A. Mee, C. F. Osborne. Macquarie University DICTA 93, 1993. pp 666-673.

4 Ravi, K. Data Security and Authentication Using Steganography / Kumar Ravi, Murti. P. R. K, International Journal of Computer Science and Information Technologies Vol. 2 (4), IJCSIT, 2011. pp 1453-1456.

5 Chang-Chou, L. Secret image sharing with steganography and authentication / Chang-Chou Lin, Wen-Hsiang Tsai, Journal of Systems and Software, Volume 73, Issue 3. ELSEVIER, 2004. pp 405-414.

6 ГОСТ Р 9594-8-98. Информационная технология. Взаимосвязь открытых систем. Справочник. Часть 8. Основы аутентификации. М. : Стандартинформ, 1999.

7 Конахович, Г. Ф. Компьютерная стеганография. Теория и практика / Г. Ф. Конахович, А. Ю. Пузыренко. МК-Пресс, 2006.

8 Banerjee, D. Asymmetric Key Steganography / Debrup Banerjee. 2011 International Conference on Information and Electronics Engineering IPCSIT vol.6, IACSIT Press, 2011.

9 Von Ahn, L. Public-Key Steganography / Luis von Ahn, Nicholas J. Hopper. Proceedings of Eurocrypt 2004. Springer, 2004.

10 Simmons, G. J. The Prisoners' Problem and the Subliminal Channel / Gustavus J. Simmons, David Chaum. Advances in Cryptology, Proceedings of Crypto 83. Springer, 1983. pp 51-67.

11 Ватолин, Д. Методы сжатия данных. Устройство архиваторов, сжатие изображений и видео / Д. Ватолин, А. Ратушняк, М. Смирнов, В. Юкин. М: ДИАЛОГ-МИФИ, 2003.

12 Сэломон, Д. Сжатие данных, изображений и звука / Д. Сэломон. М: Техносфера, 2004.

13 Westfeld, A. F5 — A Steganography Algorithm / Andreas Westfeld. 4th International Workshop, Springer, 2001.

14 Garg, T. A Review on Data Compression Using Steganography / Tamanna Garg, Sonia Vatta. International Journal of Computer Science and Mobile Computing, vol. 3 Issue 6, 2014, pp. 275 – 278.