В ближайшее время блокчейн будет встроен в бесчисленное количество мобильных приложений, от розничной торговли до финансов, цепочки поставок и многих других отраслей. Это обеспечит безопасные мобильные варианты для этих секторов или отраслей. Однако разработчики должны понимать, что для интеграции технологии блокчейн в свой проект им сначала необходимо поставить четкие цели использования блокчейна в конкретном случае. Включение технологии блокчейн в проект разработки приложений - непростая задача, но еще сложнее сделать их безопасными. Квалифицированных разработчиков мобильных приложений, которые хорошо разбираются в разработке приложений с блокчейном, в отрасли по-прежнему не хватает. Таким образом, очень важно установить правильные стандарты и использовать правильные инструменты для поощрения большего числа разработчиков к участию в этой сфере.

ЛИТЕРАТУРА

1. Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World by Don and Alex Tapscott – 2016.

2. Quytech [Электронный ресурс] - Режим доступа: https://www.quytech.com/blog/blockchain-development-complete-guide-to-getting-started/ (дата обращения 15.04.2022).

УДК [004.056+003.26](075.8)

Студ. Д.В. Божко
Науч. рук. проф. П.П. Урбанович
(кафедра информационных систем и технологий, БГТУ)

СТЕГАНОГРАФИЯ В ЗАЩИТЕ ИНФОРМАЦИИ. СРАВНЕНИЕ СТЕГАНОГРАФИЧЕСКИХ МЕТОДОВ

Способы и методы скрытия секретных сообщений в других сообщениях относятся к научному направления, которое называется «стеганография». Основная суть ее заключается в том, чтобы скрыть не только саму информацию, но еще и факт ее передачи, замаскировав передаваемые данные в какую-нибудь обыденную информацию, факт передачи которой не вызывает никаких подозрений. В простейших случаях может быть использовано несколько подходов [1].

Стеганография используется не только для передачи данных, но и для защиты авторских прав [2]. Но может быть использована и для незаконных целей.

Стандартная стеганографическая схема сохраняется вне зависимости от технологии, которой она реализуется. При построении стеганосистемы должны учитываться следующие положения:

– противник имеет полное представление о стеганографической системе и деталях ее реализации;

– если противник узнает о факте существования скрытого сообщения, это не должно позволить ему извлечь подобные сообщения в других данных;

– потенциальный противник должен быть лишен каких-либо технических и иных преимуществ в распознавании или раскрытии содержания тайных сообщений.

В данной работе были рассмотрены такие стеганографические методы, как [1, 3]:

– LSB (метод наименее значащего бита); суть этого метода заключается в замене последних значащих битов в контейнере (тексты, изображения, аудио или видеозаписи) на биты скрываемого сообщения;

– псевдослучайные перестановки (ПП); в этом методе биты скрытого сообщения распределены по изображению случайным образом;

– метод с использованием патчей (ИП); основан на статистическом кодировании информации путем изменения некоторых статистических свойств контейнера;

– метод расширения спектра (РС); здесь скрытое сообщение распределяется по контейнеру, что затрудняет выявление стеганограммы; он комбинирует расширение спектра, кодирование с исправлением ошибок и обработку изображений для скрытия вставляемого сообщения;

– дискретное косинус-преобразование (ДКП); одна из идей стеганографии состоит в том, что скрытое сообщение маскируют заменой несущественных параметров изображения, но в формате JPEG в процессе сжатия возможно изменение или даже удаление таких параметров.

– дискретное вейвлет-преобразование (ДВП); вейвлет-преобразования широко применяются в обработке сигналов и сжатии изображений; ввиду возможности анализа сигнала в выделенном интервале спектра они являются мощным инструментом для исследования особенностей поведения сигнала на различных частотных интервалах.

Было проведено сравнение вышеупомянутых методов с помощью определенных критериев, таких как уровень восприятия, вмести-

мость (пропускная способность), робастность (для защиты от статической атаки и для защиты от целенаправленного повреждения), способность к обнаружению, вид области, независимость от формата.

После проведенных исследований были сделаны выводы относительно каждого стеганографического метода. Все основные форматы графических файлов (методы тестировались именно на них) имеют различные методы сокрытия сообщений со своими сильными и слабыми сторонами. Выбор метода с большой надежностью противостоит методу с высокой скоростью обработки. Например, патч-подход имеет очень высокую устойчивость по отношению к большинству видов атак, но он может скрыть лишь очень небольшое количество информации. Поэтому более разумно скрывать информацию в дополнительных преобразованиях, а не в исходных файлах. ДВП более надежно, потому что позволяет скрыть сообщение в области частот. Данная область менее подвержена зрению человека.

ЛИТЕРАТУРА

1. Урбанович, П. П. Защита информации методами криптографии, стеганографии и обфускации: учеб.-метод. пособие / П.П. Урбанович. – Минск: БГТУ, 2016. – 220 с.

2. Шутько, Н. П. Моделирование стеганографической системы в задачах по охране авторских прав / Н.П. Шутько, Н.И. Листопад, П.П. Урбанович // Восьмая Междунар. научно-техн. конф. «Информационные технологии в промышленности» (ITI`2015): тезисы докладов. – Минск: ОИПИ НАН Беларуси, 2015. – С. 30–31.

3. Сайеди, С. А. Сравнение методов стеганографии в изображениях / С. А. Сайеди, Р. Х. Садыхов // Информатика. – 2013. – №1. – С. 66–75.

УДК [004.056+003.26](075.8)

Студ. Т.С. Белявский, А.П. Пулатов
Науч. рук. проф. П. П. Урбанович
(кафедра информационных систем и технологий, БГТУ)

ИСПОЛЬЗОВАНИЕ ХЕШ-ФУНКЦИИ SHA-256 В КРИПТОВАЛЮТНОМ АЛГОРИТМЕ BITCOIN

Криптографическая хеш-функция – это функция, реализующая алгоритм, выполняющий проверку целостности данных, защиту файлов, а также аутентификацию на основе использования математических преобразований, которые преобразовывают массив данных в состоящую из букв и символов строку фиксированной длины.