УДК 004.056.5
DOI: 10.31673/2409-7292.2020.015800

Борисенко И.И., Трифонова Е.А.

СИСТЕМА ПЕРЕДАЧИ СЕКРЕТНЫХ ДАННЫХ ОСНОВАННАЯ НА КРИПТО-СТЕГАНОГРАФИЧЕСКОЙ ТЕХНИКЕ

В статье предложен подход к улучшению стеганостойкости алгоритмов сокрытия информации за счет совместного использования криптографических преобразований информации со стеганографическими. Дана оценка качества криптостеганографических систем.

Ключевые слова: стеганография, криптография, секретные данные, передача данных, цифровое изображение.

Введение

Беспрерывно возрастающие возможности современных коммуникаций требуют все более новых специальных средств безопасности. Проблема несанкционированного копирования цифровых носителей вызывает большое беспокойство. Для преодоления этой проблемы созданы и продолжают развиваться методы сокрытия информации в основу которых положена техника встраивания конфиденциальных данных в цифровые медиа таким образом, что извлечение этих данных не может быть легким без специализированной техники.

Существует ряд способов для обеспечения безопасности данных. Один из них это криптография. В современных условиях методы традиционной криптографии в целом ряде задач становятся недостаточными, поскольку не позволяют сохранить в тайне сам факт передачи и/или хранения информации, ее объем и источник. Решением подобных проблем может быть сокрытие самого факта передачи информации. Методы стеганографии позволяют скрытно внедрять конфиденциальную информацию в компьютерные данные. Эффективное решение этих задач говорит о целесообразности разработки стеганографических систем.

С другой стороны, поскольку принято считать, что стеганосистема должна обеспечивать защиту сообщения при условии, что стеганоалгоритм полностью известен потенциальному противнику [1], то надежность сокрытия факта внедрения сообщения должна обеспечиваться организацией в стеганосистеме внутренней криптозащиты с использованием секретного ключа. Алгоритм внутренней криптозащиты может быть создан на базе теоретически обоснованных методов шифрования в соответствии с действующим законодательством конкретной страны, государственным статусом пользователя стеганосистемы, объявленными им целями применения стеганосистемы и требуемой эффективностью внутренней криптозащиты системы.

Большинство существующих стеганографических алгоритмов оперируют входными данными вне зависимости от их статистических характеристик. В действительности же распределение входных данных для стеганографических алгоритмов играет очень важную роль. В [2] предложен метод количественной оценки возмущений контейнера при его стеганографическом преобразовании, который позволяет построение более эффективных алгоритмов за счет минимизации влияния встроенного сообщения на контейнер.

Цель статьи и постановка задач

Целью данной работы является повышение надежности стеганографической системы за счет применения предварительной криптозащиты конфиденциальной информации встраиваемой в цифровое изображение.

Для достижения поставленной цели необходимо решить следующие *задачи*:

1) разработать криптографический алгоритм шифрования конфиденциальной информации встраиваемой в изображение;

2) выбрать стеганографический алгоритм встраивания шифрограммы в изображение-контейнер;

3) обеспечить контроль целостности передаваемого сообщения;

4) построить крипто-стего систему передачи данных;

Основная часть

Одной из центральных задач арифметики остатков является решение уравнения:

$$a \times x = b (\mathrm{mod} n), \quad (1)$$

т.е. поиска элемента *x*, который удовлетворяет этому уравнению. Такое уравнение может иметь одно решение, несколько, или не иметь решений. Для криптографии имеет интерес именно первый случай. Если наибольший общий делитель (НОД) НОД (a, *n*) =1, то имеем одно решение. Примером может служить уравнение 7x=3(mod143). Решая уравнение (1) мы приходим к вопросу о существовании *мультипликативного обратного* у числа *a* по модулю *n*.

Вычисление мультипликативного обратного числа. Мультипликативным обратным числом к числу A по модулю *n* будем называть такое число A^{-1}, что (AA^{-1}) mod n = 1. Решение такой задачи существует только тогда, когда A и n взаимно простые числа, т.е. НОД(A, *n*) =1. Для нахождения A^{-1} будем использовать расширенный алгоритм Евклида [3].

Расширенный алгоритм Евклида. Обозначим *r*0=*a*, *r*1= *b*, *r*m= НОД(*a*,*b*) *r*2= *r*0-q1*r*1= *a*-q1*b*, *r*3= *r*1- q2 *r*2= *b*- q2(*a*- q1*b*)=- q2*a*+(1+ q1q2)*b*, *r*4= *r*2- q3 *r*3= *a*- q1*b*- q3(- q2*a*+(1+ q1q2)*b*)= *a*- q1*b*+ q3q2*a*- q3*b*- q1q2q3*b*= (1+q2q3)*a*-(q1+ q3+ q1q2q3)*b*, *r*m =$s_m a+t_m b$. Таким образом r_m = НОД(a, *b*) =$s_m a+t_m b$.

Пример. Найти обратный к 7 по модулю 143. Положим *r*0=143, *r*1=7, тогда *r*2=143-7*20=3 *r*3=7-3*2=7-(143-7*20)*2=-143*2+7*41=1. Таким образом 7^{-1}=41(mod143).

Криптографический алгоритм cryptomatrix. В качестве примера рассмотрим «АСТ», ключ K=«GYBNQKURP» и модуль криптосистемы 26. Занумеруем буквы латинского алфавита, начиная с нуля. Ключ К представим в матричном виде: $K=\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix}$. Данная матрица обратима, так как ее детерминант не равен нулю и не имеет общих делителей с основанием модуля. Опасность того, что детерминант матрицы ключа будет иметь общие делители с модулем криптосистемы, может быть устранена путем выбора простого числа как модуля.

Сообщение представим в виде вектора S, в общем случае в виде матрицы, размерность которой совпадает с размерностью матрицы ключа: $S=\begin{pmatrix} 0 & 2 & 19 \end{pmatrix}$. Тогда зашифрованный текст получим перемножением матрицы ключа на вектор сообщения: C = KS(mod 26) = $\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix}\begin{pmatrix} 0 \\ 2 \\ 19 \end{pmatrix}$ (mod 26) = $\begin{pmatrix} 15 \\ 14 \\ 7 \end{pmatrix}$. Матрица ключа К обратима, поэтому можем найти K^{-1} по модулю 26. Отличие нахождения просто K^{-1} от K^{-1} по модулю m состоит в том, что результаты всех вычислений приводятся к остатку от деления на m, а операция деления на детерминант заменяется на операцию умножения на обратный к значению детерминанта в кольце по модулю элемент. Обратный элемент по модулю находим, используя расширенный алгоритм Евклида. Итак, K^{-1} (mod 26) = $\begin{pmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{pmatrix}$. Восстановление исходного текста S: S = K^{-1}C (mod 26) = $\begin{pmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{pmatrix}\begin{pmatrix} 15 \\ 14 \\ 7 \end{pmatrix}$ (mod 26) = $\begin{pmatrix} 0 \\ 2 \\ 19 \end{pmatrix}$.

В настоящее время на рынке программных продуктов можно встретить достаточное количество стеганопрограмм. В большинстве из них применяются различные модификации LSB-метода, обладающие значительным количеством недостатков. В [4] был предложен стеганографический алгоритм Stego_Graph организации пересылки и декодирования секретной информации, основанный на применении теории графов. Stego_Graph был модифицирован с целью повышения его помехоустойчивости [5]. Идея стеганоалгоритма Stego_Graph состоит в том, чтобы одну бинарную последовательность, выполняющую роль секретного сообщения (СИ) погрузить в другую бинарную последовательность - контейнер путем сравнения битов СИ с битами контейнера, определяющих в нем в дальнейшем локализацию СИ. В случае несовпадения соответствующих битов СИ и контейнера производиться корректировка элементов контейнера с целью приведения их к бинарному виду СИ. В дальнейшем будем использовать Stego_Graph [5].

Хеширование. Хеширование - преобразование исходных данных произвольной длины в выходную строку фиксированной длины, которую будем называть хешем. Для стеганографических целей очень важно, чтобы скрытое сообщение сохранило свою целостность и если сообщение модифицировалось третьим лицом, то получатель должен обнаружить это. Простым решением этой проблемы является то, что кроме основного сообщения мы будем погружать и его хешированную версию, которая обычно короче оригинального сообщения. Для хеширования данных используется 128 -битовый алгоритм MD5.

Построение крипто-стего системы Cript_steg. Крипто–стего система в общем виде представлена на рисунке 1.

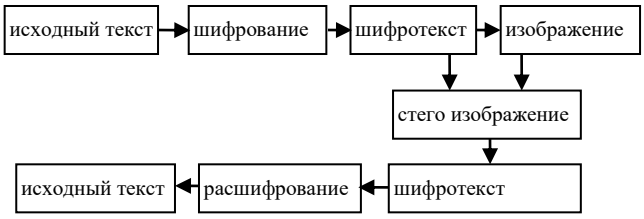

Рис. 1 Схема крипто–стего системы

Чтобы скрыть исходный текст (сообщение) в выбранном изображении следует выполнить следующие шаги.

1. Шифруем исходный текст алгоритмом *cryptomatrix*, получаем шифротекст *shifr*
2. Создаем хешированную версию *hesh* для исходного текста алгоритмом MD5
3. Внедряем в выбранное изображение файлы *shifr* и *hesh* алгоритмом Stego_Graph, получаем стегоизображение *steg*, которое пересылается получателю.

В *steg* могут быть внедрены также криптографический ключ и стегоключ, которым является размер блока в алгоритме Stego_Graph.

Для извлечения данных получатель выполняет шаги.

1. Из стегоизображения *steg* извлекается шифротекст и файл *hesh* алгоритмом Stego_Graph
2. Зная криптографический ключ получатель расшифровывает шифротекст алгоритмом *cryptomatrix*
3. Вычисляется хеш алгоритмом MD5 для расшифрованного текста, полученного на предыдущем шаге
4. Если хеш, полученный на шаге 3 совпал с извлеченным на шаге 1 файлом *hesh*, то при пересылке оригинальное сообщение не подвергалось модификации

Выводы

Таким образом, разработана криптостегосистема Cript_steg для повышения безопасности информационных систем путем объединения двух техник – сначала сообщение шифруется, а затем шифротекст погружается в выбранное изображение. Контроль целостности пересылаемого сообщения осуществляется путем вычисления его хеша. В основу Cript_steg положен шифр *cryptomatrix*, разработанный в данной работе и стегоалгоритм Stego_Graph, разработанный авторами ранее.

Список использованных источников

1. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. – М.: Солон-Пресс, 2002. – 272 с.

2. Борисенко І.І. Оценка возмущения контейнера при его стеганопреобразовании / І.І. Борисенко// Високі технології в машинобудуванні – 2015. – №1. – С. 27-32.

3. Н. Смарт Криптография – М.: Техносфера. – 2006. – 525 с.

4. Борисенко И.И. Особенности применения многоуровневого порогового преобразования изображения в компьютерной стеганографии/ И.И.Борисенко// Праці УНДІРТ. Теоретичний та науково-практичний журнал радіозв'язку, радіомовлення і телебачення, 4(48) 2006. Видання УНДІРТ м. Одеса – с.53-59.

1. Борисенко И.И. Повышение помехоустойчивости стеганографического алгоритма/ И.И.Борисенко// Сучасний захист інформації. – 2010. – №1. – С. 36–42

Надійшла: 31.01.2020 Рецензент: д.т.н., професор Гайдур Г.І.