УДК 004.056.55

УСИЛЕНИЕ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ СОЧЕТАНИЕМ КРИПТОГРАФИЧЕСКИХ И СТЕГАНОГРАФИЧЕСКИХ МЕТОДОВ ЗАЩИТЫ

Воротникова Ю.А., Чернышова А.В.
Донецкий национальный технический университет, Украина

Рассмотрена комбинация криптографических и стеганографических средств защиты информации. Описывается подход сокрытия информации в изображениях формата BMP. Обосновывается необходимость предварительного шифрования данных перед применением стеганографических алгоритмов. Рассмотрен алгоритм сокрытия изображения формата BMP в трех изображениях того же формата.

Введение

В современном мире большое количество важной и секретной информации хранится на электронных носителях и пересылается по сетям. Это открывает широкие возможности для злоумышленников, желающих получить секретную или конфиденциальную информацию пользователей. С целью предотвращения утечки и кражи информации разработано огромное количество криптографических и стеганографических средств защиты информации.

1 Обоснование необходимости шифрования данных перед применением стеганографических алгоритмов

Стеганографические алгоритмы являются не самым надежным средством защиты информации в случае, когда злоумышленник знает, что некоторый мультимедийный файл (в нашем случае - графический) содержит в себе спрятанную информацию. В частности, если данные зашифрованы в изображение по методу LSB, то противнику точно известно, где искать спрятанные данные [1].

Для решения данной проблемы можно использовать предварительное шифрование данных, которые записаны в изображение. Это позволит повысить надежность криптосистемы и снизить риск дешифрования информации.

В качестве алгоритма шифрования целесообразно выбирать симметричные алгоритмы, поскольку они обеспечивают хорошую криптостойкость, а также просты в реализации. В данной работе в качестве симметричного алгоритма шифрования данных используется XTEA. Это блочный алгоритм, основан на операциях с 64-битным блоком, имеет 32 полных цикла, в каждом полном цикле по два раунда Сети Фейстеля, что означает 64 раунда сети Фейстеля [2,3,4]. Данный алгоритм наиболее уязвим к дифференциальным атакам. Для случая с последующим применением стеганографического алгоритма шифрования данных, алгоритм XTEA обеспечивает высокую криптостойкость.

2 Описание стеганографичсекого алгоритма сокрытия данных в изображении

В качестве контейнера для хранения зашифрованного сообщения выбирается 24-битное изображение в формате BMP. Суть алгоритма состоит в том, что каждый байт зашифрованного сообщения разбивается на последовательность бит, каждый из которых записывается в седьмой бит одного из цветовых компонент (R, G или B) очередного пикселя. Пиксели можно выбирать как подряд, так и с некоторым интервалом. Для обеспечения возможности корректного дешифрования данных в начало изображения записывается 32-битное значение размера данных. Оба варианта имеют недостатки, т.к. в случае перехвата изображения с зашифрованными данными противник будет видеть количество и расположение зашифрованной информации, поскольку при использовании седьмого бита цвет пикселя искажается. Наилучшим вариантом является сокрытие такого количества текста в изображении, которое оно максимально может в себя вместить. Тогда противник получит зашумленное изображение (внешне напоминает применение некоторого фильтра) и, возможно, не

догадается о наличии в нем зашифрованного текста. Для случая с выбором каждого пикселя для помещения в него одного бита информации, максимальный объем вмещаемых байт информации N рассчитывается по формуле (1).

$$N = \frac{xSize * ySize}{8} - 4, \quad (1)$$

где xSize – горизонтальное разрешение изображения, ySize – вертикальное разрешение изображения. Четыре байта занимает размер данных.

Для случая с выбором пикселей через некоторые интервалы dx, dy максимальный объем вмещаемых байт информации N рассчитывается по формуле (2).

$$N = \frac{xSize}{dx+1} * \frac{ySize}{dy+2} - 4, \quad (2)$$

где xSize – горизонтальное разрешение изображения, ySize – вертикальное разрешение изображения, dx – интервал выбора пикселей по горизонтали, dy – интервал выбора пикселей по вертикали.

3 Описание алгоритма сокрытия изображения

После шифрования секретного сообщения алгоритмом XTEA и сокрытия результирующего шифротекста в изображении применяется алгоритм сокрытия этого изображения в трех контейнерах формата BMP. Основой для разработки алгоритма послужил метод LSB. Известно, что человек обычно не способен заметить изменение в последнем бите. Фактически, он является шумом. Поэтому последние биты можно использовать для встраивания информации. Таким образом, для полутонового изображения объем встраиваемых данных может составлять 1/8 объема контейнера. Если модифицировать два младших бита (что также почти незаметно), то можно скрытно передать вдвое больший объем данных [5].

Суть алгоритма заключается в том, что секретное изображение разбивается на три цветовых примитива (то есть на оттенки красного, зеленого и синего), а затем каждый примитив записывается в младшие биты одного из изображений-контейнеров. Таким образом, после зашифровки каждый контейнер будет содержать в себе одну цветовую составляющую секретного изображения.

Из каждого цветового примитива берется два старших бита и записывается в младшие биты соответствующего цвета у соответствующего контейнера. Два младших бита в двух оставшихся цветах обнуляются. Операция повторяется для каждого пикселя. Изображения-контейнеры визуально не теряют в качестве, т.к. изменение младших битов цвета не ощутимо для человеческого зрения.

Для восстановления изображения берем пиксель из каждого изображения-контейнера. Два младших бита каждого цвета в этом пикселе делаем старшими битами и складываем соответствующие цветовые составляющие. Поскольку во время сокрытия изображения в трех изображениях младшие биты не шифруемого цвета обнулялись, то ненулевое значение будет иметь только одна цветовая составляющая в каждом контейнере. Таким образом, можно восстановить цвет соответствующего пикселя секретного изображения (с некоторой погрешностью). Далее повторим эту операцию для всех пикселей и получим восстановленное секретное изображение.

Восстановленное изображение существенно потеряло в качестве (из 24-битного оно превратилось в 6-битное), однако оно содержит всю необходимую нам информацию для извлечения зашифрованного симметричным алгоритмом секретного сообщения.

На рис. 1 представлена общая схема шифрования сообщения трехступенчатым алгоритмом, включающим в себя криптографические и стеганографические методы защиты информации.

При дешифровании сообщения схема работает в обратную сторону. Схема работы криптосистемы при дешифровании представлена на рис. 2.

Один из недостатков алгоритма - для извлечения закодированного сообщения нужны все три изображения. Если какого-либо изображения не хватает, либо если изображение частично или полностью искажено, то извлечение зашифрованного изображения становится невозможным. Необходимым требованием также является точное совпадение разрешений используемых

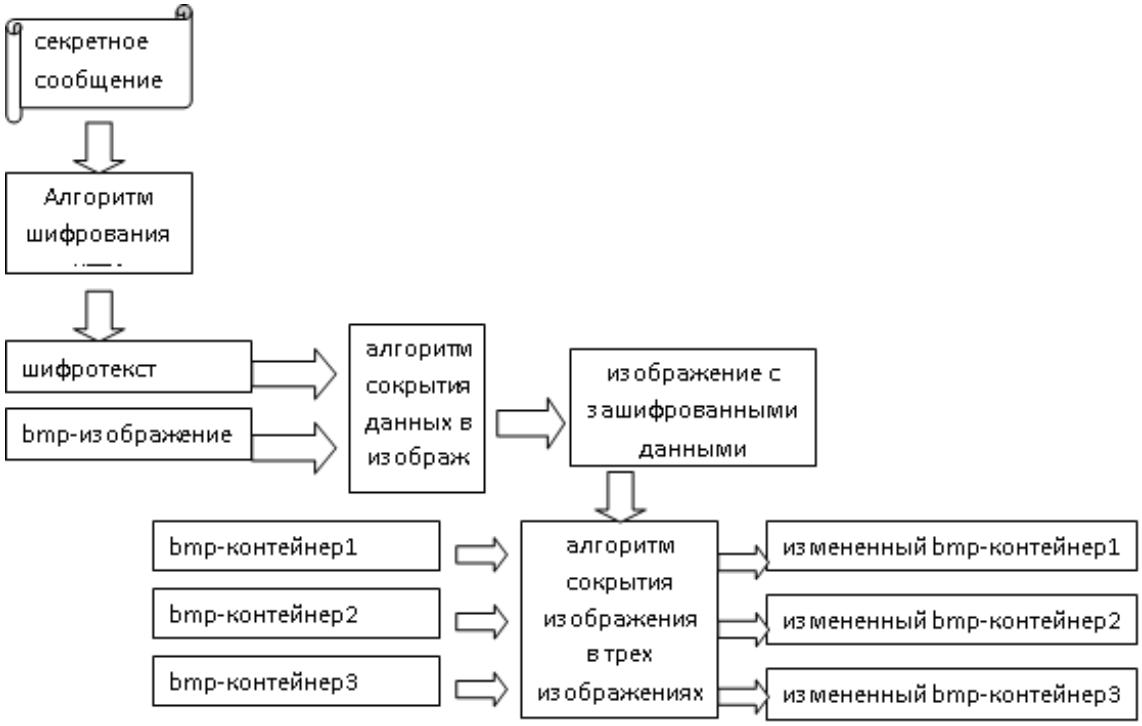

Рисунок 1. Общая схема шифрования сообщения

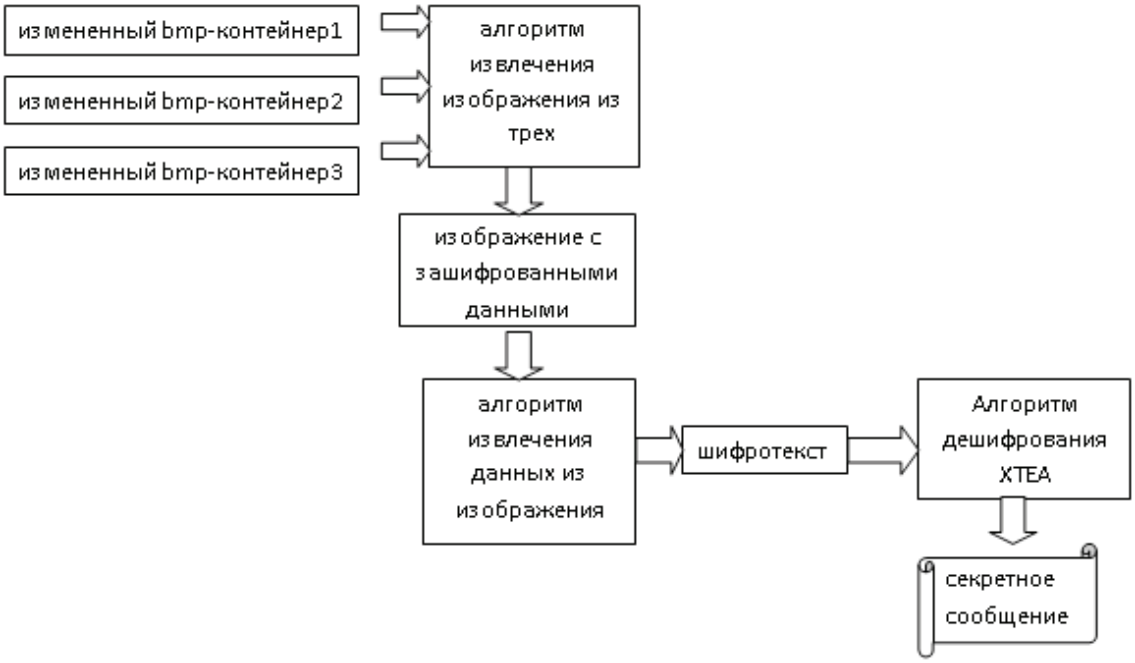

Рисунок 2. Общая схема дешифрования сообщения

изображений, иначе дешифрование изображения из трех других будет произведено некорректно.

Вторым недостатком рассмотренного алгоритма является то, что необходимо продумать и реализовать дополнительные средства защиты ключа симметричного алгоритма, поскольку для шифрования и дешифрования в симметричных криптосистемах используется один ключ. Одним из вариантов может быть шифрование ключа симметричного алгоритма с помощью ассиметричного алгоритма RSA и дальнейшую передачу ключа по открытым каналам без использования стеганографических методов защиты. Другой вариант – сокрытие ключа в изображении вместе с зашифрованными данными. Однако этот способ небезопасен для случая, если данные будут перехвачены злоумышленником.

Как достоинством, так и недостатком можно считать сложную многоступенчатую схему

шифрования-дешифрования секретного сообщения. Достоинство состоит в том, что при попадании результирующих изображений к злоумышленнику, извлечение сообщения становится практически невозможным при отсутствии полной информации о применяемых методах. Однако сложность алгоритма затрудняет дешифрование данных, а при потере или искажении изображений-контейнеров делает его невозможным.

4 Выводы

Трехступенчатый алгоритм, включающий в себя как криптографические, так и стеганографические методы защиты информации, позволяет с большой степенью надежности шифровать секретные сообщения достаточно большого объема. Комбинация различных методов позволяет повысить криптостойкость всего алгоритма в целом.

Литература

[1] Стеганография. Материал из Википедии – свободной энциклопедии. Электронный ресурс. Режим доступа: http://ru.wikipedia.org/wiki/Стеганография

[2] XTEA. Материал из Википедии – свободной энциклопедии. Электронный ресурс. Режим доступа: http://ru.wikipedia.org/wiki/XTEA

[3] Сеть Фейстеля. Материал из Википедии – свободной энциклопедии. Электронный ресурс. Режим доступа: http://ru.wikipedia.org/wiki/Сеть_Фейстеля

[4] Хорст Файстель. Криптография и компьютерная безопасность. Перевод Андрея Винокурова.

[5] Грибунин В. Г., Оков И. Н., Туринцев И. В. Цифровая стеганография. — М.: Солон-Пресс, 2002. — 272 с, ил.