Ссылка на статью:
// Ученые записки УлГУ. Сер. Математика и информационные технологии. УлГУ. Электрон. журн. 2017, № 1, с.10-12.

Поступила: 03.09.2017
Окончательный вариант: 04.10.2017

© УлГУ

УДК 004.056.5

Стеганографический метод передачи информации, не вызывающий искажений контейнера

Валеев Д. М.[1,*]

[*] damirivaleev@gmail.com
[1]УлГУ, Ульяновск, Россия

Предложен метод стеганографической передачи данных с использованием ключевой информации, который не позволяет обнаружить встроенное секретное сообщение внутри стегоконтейнера. Описан алгоритм встраивания сообщения, создания ключевой информации, а также алгоритм извлечения сообщения из стегоконтейнера. Обсуждается применение данного метода к цифровым водяным знакам.

Ключевые слова: *стеганография, ключ, встраивание, цифровые водяные знаки*.

В информационном пространстве постоянно появляются и улучшаются методы обработки, хранения и передачи информации, в том числе и методы скрытой передачи данных. Такая передача является угрозой для возникновения каналов передачи информации злоумышленников. Чтобы обезопаситься от таких угроз, приходится изучать эти методы и находить способы закрыть уязвимые места, которые используют эти методы скрытой передачи информации. В данной работе предлагается исследовать такой метод.

Следуя общепринятой терминологии, будем использовать термин контейнер для обозначения информации, в которую встраивается другая информация для скрытой передачи по каналу связи. Секретное сообщение – та информация, которую встраивают в контейнер. Встраивание – процесс преобразования контейнера с помощью секретного сообщения таким образом, чтобы сообщение можно было передать по каналу связи незаметно для злоумышленника. Однако стоит сделать уточнение: в нашем методе не используется встраивание как таковое, поэтому будем использовать термин «встраивание» с использованием кавычек. Стегоконтейнер – контейнер, содержащий встроенное сообщение. Также

в данном методе используется секретный ключ – информация, которая используется в процессе встраивания и содержится в секрете от злоумышленника.

В основе метода лежит алгоритм, похожий на использование трафарета, который с древних времен применялся для тайных коммуникаций между лицами, знающими и договорившимися о действии трафарета. Они использовали всем известную книгу, например Библию, в качестве основы для обмена сообщениями. Материалом для ключевой информации служил лист бумаги с отверстиями в определенных местах, положив который на страницу книги, можно было прочесть сообщение, собрав буквы, отображающиеся через отверстия [1]. Нетрудно предположить, что такой лист бумаги должен быть защищен от противника, книгу, же защищать не нужно было.

Еще одним похожим методом была решетка Кардано. Итальянский математик Джероламо Кардано (1501 – 1576) предложил использовать лист с отверстиями для маскирования секретного сообщения в обычных посланиях. По его методу в листе проделывали отверстия, в отверстиях вписывалось сообщение, а затем из полученных фраз составляли безобидное послание [2]. В данном случае процесс придумывания осмысленного текста из набора букв и слов является трудоемким.

С развитием цифровой обработки информации стал возможным другой подход, в котором несекретное сообщение уже существует в виде контейнера. Контейнер может быть текстом, фотографией или музыкальной композицией. Его можно использовать для внедрения секретного сообщения.

Опишем метод «встраивания» секретной информации в контейнер для установления скрытого канала передачи информации.

Для работы алгоритма «встраивания» секретного сообщения необходимо преобразовать исходный контейнер в виде двоичной последовательности. Соответственно, секретное сообщение необходимо также представить в виде двоичной последовательности. Теперь можно приступить к созданию ключевой информации, которая будет выглядеть в виде однострочной таблицы, ячейки которой будут соответствовать каждому биту секретного сообщения, а информация внутри ячеек – координатам нахождения битов секретного сообщения в контейнере.

Старт алгоритма начинается с нулевых битов контейнера и секретного сообщения. -ая ячейка таблицы заполняется j-ым номером байта контейнера, если i-ый бит секретного сообщения равен старшему биту j-ого байта контейнера. Если условие выполнено, переходим к заполнению ячейки $i+1$, номер байта контейнера также становится $j+1$. Если условие не выполнено, переходим к $j+1$ байту контейнера. Таким образом, заполняются все ячейки ключевой таблицы, до тех пор, пока все секретное сообщение не будет «помещено» в контейнер. Исходя из алгоритма, размер секретной информации не может превышать $1/8$ размера контейнера, чтобы не возникло ситуации, когда алгоритм дошел до последнего байта контейнера, а секретное сообщение «встроено» не полностью.

Далее, можно направить полученный стегоконтейнер собеседнику, если не было договорённости заранее об использовании конкретного контейнера. Собеседник сможет

прочесть «встроенное» секретное сообщение, получив ключевую таблицу по защищенному каналу связи следующим образом: прочитав значение -ой ячейки ключевой таблицы, он ищет в стегоконтейнере байт, номер которого равен значению ячейки i ключевой таблицы и получает первый бит этого байта. Этот бит равен -ому биту секретного сообщения. Таким образом, восстанавливается все секретное сообщение.

Поскольку область науки сокрытия информации включает в себя не только стеганографию, но и цифровые водяные знаки (далее – ЦВЗ), данный метод можно использовать в качестве ЦВЗ для обеспечения целостности защищаемой информации и обнаружения атак на стегоконтейнер, поскольку метод использует для «встраивания» старший бит, изменение которого можно легко отследить. Однако этот метод уязвим к проблеме двойного авторства, поскольку в данном методе не происходит встраивания как такового и ничто не мешает злоумышленнику «встроить» в контейнер свою секретную информацию, претендуя на авторство контейнера. Следуя общепринятой терминологии, такой метод можно отнести к хрупким и полу-хрупким ЦВЗ.

Список литературы

1. Petitcolas F.A.P., Anderson R.J., Kuhn M.G. Information Hiding – A Survey // *Proceeding of the IEEE, special issue on protection of multimedia content.* 1999. July. №87. P. 1062-1078.
2. Цифровой водяной знак [Электронный ресурс]. Режим доступа: https://ru.wikipedia.org/wiki/Цифровой_водяной_знак (дата обращения 19.08.2017).