Евграшин Андрей Витальевич, соискатель Кафедры «Экономические и информационные системы» (ЭИС) Поволжского государственного университета телекоммуникаций и информатики (ПГУТИ). Тел. (8-846) 228-00-36.

Маслов Олег Николаевич, д.т.н., профессор, заведующий Кафедрой ЭИС ПГУТИ. Тел. (8-846) 271-06-24; 228-00-36. E-mail: maslov@psati.ru

Рябушкин Аркадий Викторович, инженер Кафедры «Мультисервисные сети и информационная безопасность» ПГУТИ. Тел. (8-846) 339-11-43. E-mail: ryabushkin@psati.ru

Шашенков Валерий Федорович, к.т.н., с.н.с., соискатель Кафедры ЭИС ПГУТИ. Тел. (8-846) 228-00-36.

УДК 004.056

ЗАЩИТА ОТ ПЕРЕДАЧИ СТЕГОСООБЩЕНИЙ В ГРАФИЧЕСКИХ ФАЙЛАХ

Ажмухамедов И.М., Колесова Н.А.

Предложена система защиты от передачи стегосообщений в изображениях, позволяющая идентифицировать графический файл, подозрительный на содержание скрытого сообщения, в условиях отсутствия априорных сведений о наличии стего в данном файле и о законе его встраивания, а также модифицировать такое изображение с дальнейшим исключением возможности извлечения из него стегосообщения.

Ключевые слова: защита информации, графический файл, стеганография, стегосообщение, младшие биты пикселя, последовательность случайных чисел.

Введение

Развитие средств вычислительной техники в последнее десятилетие дало толчок развитию компьютерной стеганографии. Методы стеганографии, в отличие от методов криптографии, позволяют скрыть не только само сообщение, но и факт его передачи. В свою очередь бурное развитие IT-технологий и цифровых аппаратно-программных средств способствовало появлению новых возможностей для цифровой стеганографии, позволяющей встраивать сообщения в цифровые данные. При этом в качестве цифровых контейнеров используются данные, как правило, имеющие аналоговую природу: речь, аудиозаписи, видео, графические изображения, текстовые файлы и исполняемые файлы программ [1].

Наиболее распространенными являются методы встраивания скрытой информации в графические файлы [2]. Используя такие контейнеры, можно встраивать в них не только текстовую информацию, но и изображения, и другие файлы. Единственным условием является то, что объем скрываемого сообщения не должен превышать определенную величину, определяемую объемом изображения, контейнера. Для достижения этой цели используются различные методики, но все они сводятся к замене определенных пикселей в изображении.

Реальные графические образы позволяют передавать большие объемы информации. Так, для графического контейнера размером 1024×768 пикселей при использовании метода наименьшего значимого бита [3] можно передать до 98304 байт скрытой информации. При этом человеческий глаз не замечает различий между исходным и преобразованным изображениями.

При использовании стеганографических методов не только неизвестен сам факт передачи скрытой информации, но и алгоритм внедрения скрытой информации в контейнер, а также способ кодирования информации. Поэтому на сегодняшний день такие методы весьма распространены и часто используются злоумышленниками при обмене информацией.

В настоящее время разработано несколько систем обнаружения стегосообщений, например [45]. Однако данные системы не позволяют обрабатывать «подозрительные» изображения с целью исключения возможности дальнейшего извлечения стего. Кроме того, часто они эффективно могут быть использованы только для графических файлов формата JPEG , а также требуют проведения обучения, что, в свою очередь, приводит к необходимости наличия достаточного количества цифровых изображений, содержащих скрытые сообщения, встроенные с помощью различных алгоритмов.

Среди способов борьбы с передачей стегосообщений наиболее известным является метод, согласно которому изображение обрезается по краям, что в дальнейшем значительно затрудняет или полностью исключает возможность удачного декодирования [6]. Однако подобные способы применяются ко всем изображениям

без исключения, которые потенциально могут содержать стегосообщения, что во многих случаях требует дополнительных затрат времени и средств. Кроме того, в ряде случаев при передаче изображения необходимо исключить возможное возникновение искажений. Например, при передаче графических файлов высокого качества или когда проверка целостности таких файлов используется как проверка подлинности. В подобных ситуациях использование фильтров, модифицирующих все поступающие изображения, становится невозможным, а их отключение приведет к возникновению угроз информационной безопасности.

Постановка и способ решения задачи

Необходимо разработать систему защиты от несанкционированной передачи данных в графических файлах (изображениях). Рассмотрим графическую стеганографию. Цифровое изображение представляет собой матрицу пикселей, каждый из которых имеет фиксированную размерность двоичного представления. Например, пиксели полутонового изображения кодируются 8 битами (значение яркости изменяется от 0 до 255). При этом младший значащий бит пикселя изображения несет в себе меньше всего информации, различимой глазом человека. Фактически значение младшего бита является случайным. Поэтому его часто используют для встраивания информации.

Например, в случае задания пикселя тремя цветами RGB (красный-зеленый-синий) каждый пиксель описывается тремя байтами, то есть 24 битами. Тогда при внедрении скрытой информации в виде символа A (01000001) в трех последовательных пикселях, каждый из которых описывается тремя байтами:

(00100111, 11101001, 11001000)
(00100111, 11001000, 11101001)
(11001000, 01000111, 11101001)

модификации подвергается только часть значений младших бит выбранных байтов. В результате получается

(00100111, 11101001, 11001000)
(00100110, 11001000, 11101000)
(11001000, 01000110, 11101001).

При этом модификации могут подвергаться как все младшие биты, так и младшие биты только одного цветового канала.

Статистические свойства младших бит при внедрении сообщения изменяются и с высокой долей вероятности перестают носить случайный характер. Это позволяет обнаружить факт передачи стегосообщения.

Таким образом, для обнаружения наличия стегосообщения необходимо провести анализ числовых последовательностей, состоящих из младших бит каждого цветового канала пикселей изображения. При этом если наблюдается отклонение поведения хотя бы одной из таких последовательностей от случайного, выдвигается гипотеза о возможности содержания в данном изображении скрытого сообщения. Для исключения возможности извлечения стегосообщения из такого изображения младшие биты пикселей цветового канала, для которого сформированная последовательность бит признается неслучайной, обнуляются. При этом внесенные в графический файл изменения визуально неразличимы, и обнаружить их без анализа внутренней структуры файла невозможно.

На рис.1 представлена блок-схема алгоритма выявления и модификации графических файлов, подозрительных на наличие скрытого сообщения. На блок-схеме приняты следующие сокращения: SR – последовательность младших бит R-канала пикселей изображения, SG – последовательность младших бит G-канала пикселей изображения, SB – последовательность младших бит B-канала пикселей изображения.

Оценка качества (степени случайности) последовательности, состоящей из младших бит пикселей изображения, может быть осуществлена с помощью методики, описанной в [7]. Согласно данной методике, влияние результатов различных проверок последовательности бит на общий уровень ее качества может быть представлено в виде ориентированного трехуровневого графа, имеющего одну корневую вершину и не содержащего петель и горизонтальных ребер в пределах одного уровня иерархии. На втором (нижнем) уровне расположены тесты, используемые для проверки различных характеристик последовательности бит. На уровень выше находятся основные свойства случайности: равномерность, стохастичность и независимость. И, наконец, корневой вершине нулевого уровня соответствует комплексный критерий оценки качества проверяемой последовательности. Дугам графа соответствует система весов или отношений

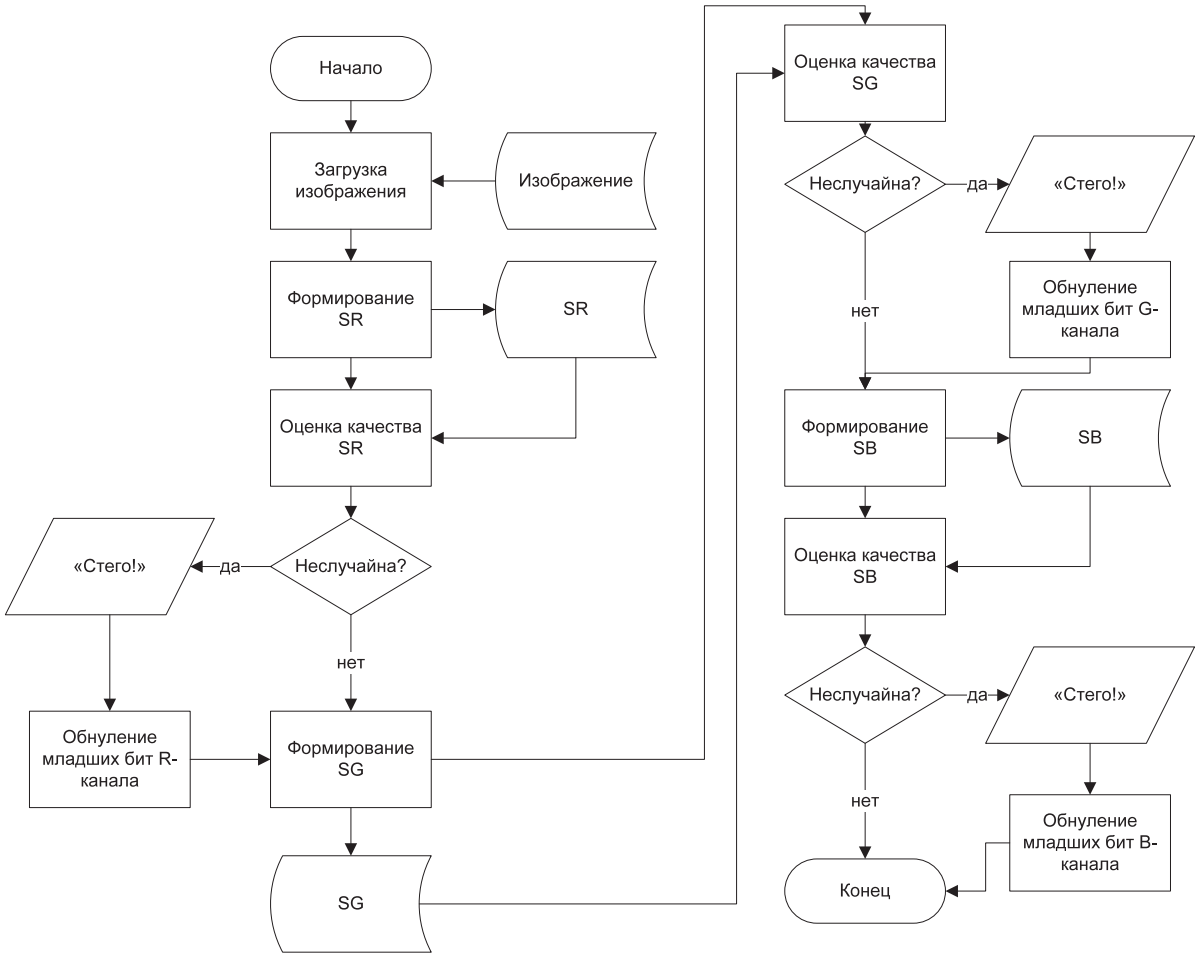

Рис.1. Блок-схема алгоритма выявления и модификации изображений, содержащих стегосообщение

предпочтения одних критериев над другими по степени их влияния на заданный элемент следующего уровня иерархии. Для комплексной оценки качества последовательности бит производится агрегирование данных, собранных в рамках иерархии. При этом агрегирование совершается по направлению дуг графа, где при переходе со второго уровня на первый применяется аддитивная свертка, а при переходе с первого уровня на нулевой – мультипликативная.

Предложенный алгоритм был положен в основу системы защиты от передачи стегосообщений в изображениях [8], общая схема работы которой представлена на рис.2.

Данная система, установленная на стороне получателя, анализирует поступающие через Интернет сообщения, содержащие графические файлы, и включает в себя следующие модули:

подсистему формирования последовательностей младших бит пикселей изображения, выделяющую в графическом файле цветовые каналы и формирующую младшие биты пикселей каждого из них в отдельную числовую последовательность;

подсистему оценки качества числовой последовательности, анализирующую поданные на вход из подсистемы (1) последовательности бит с точки зрения основных свойств случайности;

подсистему принятия решения о возможном наличии стегосообщения в изображении, работа которой основана на результатах функционирования подсистемы (2);

подсистему обнуления младших бит пикселей изображения, производящую преобразование графического файла, для которого подсистемой (3) было принято решение о возможном наличии стегосообщения.

В разработанной системе защиты от передачи стегосообщений в изображениях в качестве подсистемы оценки качества числовой последовательности используется «Программа

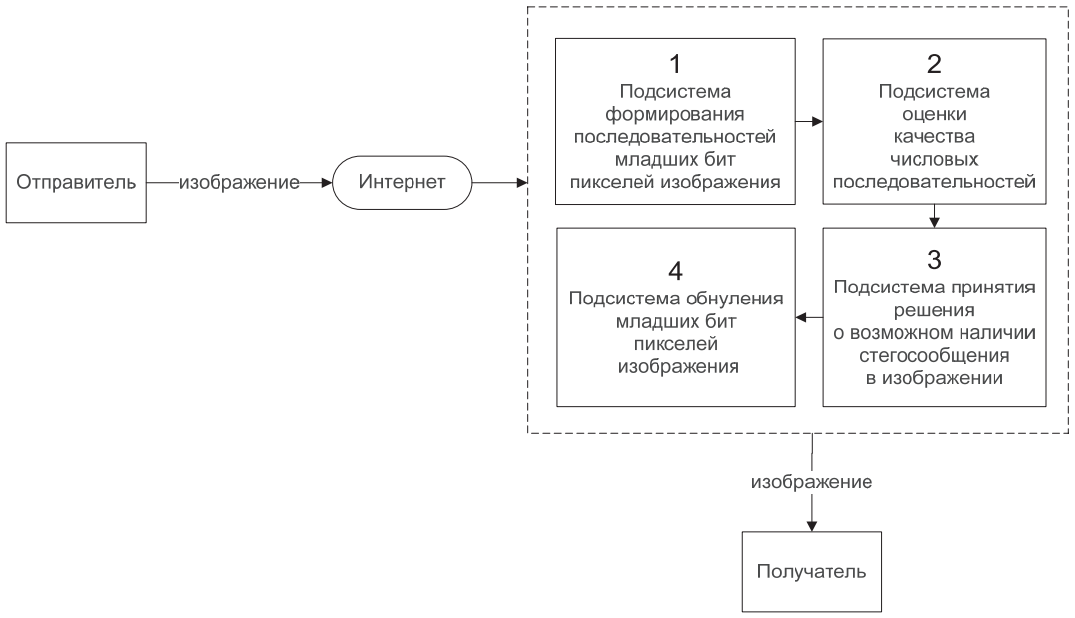

Рис. 2. Схема работы системы защиты от передачи стегосообщений в изображениях

для комплексной оценки качества последовательности случайных чисел» [9]. При этом изменение пороговых уровней и весовых коэффициентов тестов и групп тестов в указанной подсистеме может позволить изменять общий уровень защиты системы.

Предложенный подход по защите от несанкционированной передачи данных в изображениях может также быть использован и для борьбы с передачей стегосообщений, встроенных в другие цифровые контейнеры. При этом изменению подвергнется только процедура извлечения случайной последовательности из контейнера.

Пример

С целью исследования эффективности использования предложенного подхода разработанной системой было протестировано 100 графических файлов, содержащих встроенное сообщение. При этом тестирование проводилось для различных уровней защиты, характеризуемых соответствующей пользовательской стратегией:

- осторожной, при которой минимизируется ошибка 1-го рода;
- рискованной, при которой минимизируется ошибка 2-го рода;
- сбалансированной, при которой минимизируется ошибка 3-го рода,

а также значениями пороговых уровней для признания последовательности бит случайной ($\overline{\mu}_{СЛ}$) или неслучайной ($\overline{\mu}_{НС}$):

- для признания последовательности случайной, она должна пройти с положительным результатом 75% тестов, для признания неслу-

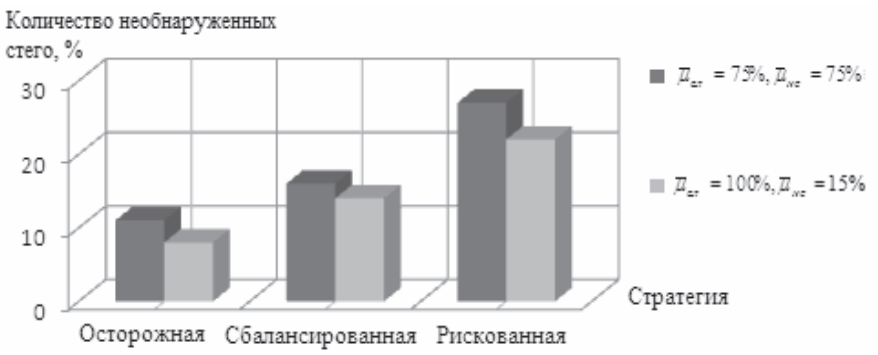

Рис. 3. Результаты фильтрации изображений, содержащих стегосообещние, при разных уровнях защиты

чайной – с отрицательным результатом 75% тестов;

- для признания последовательности случайной, она должна пройти с положительным результатом 100% тестов, для признания неслучайной – с отрицательным результатом 15% тестов.

Общие результаты тестирования приведены на рис. 3. Как видно из результатов экспериментов, разработанная система защиты от передачи стегосообщений в изображениях с высокой долей вероятности (до 92%) обнаруживает и корректирует графические файлы, содержащие скрытую информацию.

Заключение

Наличие в изображении скрытой информации может быть определено с помощью анализа последовательностей, состоящих из младших бит пикселей данного изображения, путем выявления отклонений их поведения от случайного.

Данный подход позволил разработать систему защиты от несанкционированной передачи данных в графических файлах, идентифицирующую изображения, подозрительные на содержание стегосообщения в условиях отсутствия априорных сведений о наличии скрытого сообщения и о законе его встраивания, а также модифицирующую такие изображения с дальнейшим исключением возможности извлечения из них стегосообщений.

Литература

1. Слядников Е.Е. Проблемы цифровой стеганографии // http://www.lib.tusur.ru/fulltext / analitika/conf/2004_slyadnikov_180305.pdf
2. Ярмолик С.В., Листопад Ю.Н. Стеганографические методы защиты информации // www.giac.unibel.by/sm_full.aspx?guid=7933
3. Коханович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. К.: МКПресс, 2006 – 288с.
4. Баранов В.А., Гатилов О.В., Скурнович А.В. и др. Способ поиска изображений формата JPEG, содержащих цифровой водяной знак. Патент RU 2005116628A. Опубл. 20.11.2006.
5. Иванов В.А., Стельмах Э.П., Гатилов О.В. и др. Способ идентификации цифрового изображения, содержащего цифровой водяной знак. Патент RU 2304306 C1, опубл. 10.08.2007.
6. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. М.: СОЛОНПресс, 2002. – 261 с.
7. Колесова Н.А., Ажмухамедов И.М. Методика оценки качества последовательности случайных чисел // Вестник АГТУ. Серия «Управление, вычислительная техника и информатика». №2, 2010. – С. 141148.
8. Система защиты от передачи стегосообщений в изображениях. Патент на полезную модель №114193. Колесова Н.А., Ажмухамедов И.М. Зарег. в Госреестре РФ 10.03.2012.
9. Свидетельство об официальной регистрации программы для ЭВМ №2010614210. Программа для комплексной оценки качества последовательностей случайных чисел. Колесова Н.А., Ажмухамедов И.М. Зарег. в реестре программ для ЭВМ 30.06.2010.

PROTECTION OF TRANSFER STEGAMESSAGES IN IMAGES

Azhmuhamedov I.M., Kolesova N.A.

Proposed the system of protection transmission stegomessages in images, allowing to identify the image file, the contents of a suspect a hidden message, in the absence of a priori information about the presence in the stego file and the law of its incorporation, and modify images with a further possible exception of the extraction stegomessages.

Keywords: *information security, image, steganography, stegomessage, least significant bits of the pixel, the sequence of random numbers.*

Ажмухамедов Искандар Маратович, к.т.н., доцент Кафедры «Информационная безопасность» (ИБ) Астраханского государственного технического университета (АсГТУ). Тел. (8-512) 61-45-10. E-mail: aim_agtu@mail.ru

Колесова Наталья Александровна, ассистент Кафедры ИБ АсГТУ. Тел. (8-512) 61-45-10. E-mail: sangreal_88@inbox.ru