$$\overline{Y_c} = x_8 \cdot [x_6 \cdot [x_3 \cdot [x_2 \cdot x_1] \cdot (x_4 \cdot x_5) \cdot x_7] \quad (3)$$

Рассмотренная примитивная СЗИ будет работать только в случае работоспособности всех элементов и совершения заданных событий. Модифицируя СФЦ, можно получить несколько сценариев исполнения основных функций СЗИ – начиная режимом полного функционирования до режима аварийной работы.

Таким образом, на данном этапе оценки «живучести» СЗИ была получена математическая модель функционирования элементов системы.

Литература

1. Можаев А.С. Теоретические основы общего логико-вероятностного метода автоматизированного моделирования систем / А. С. Можаев, В. Н. Громов. – СПб. : ВИТУ, 2000. – 145 с.

2. Синтез и анализ живучести сетевых систем : монография / Ю.Ю. Громов, В. О. Драчев, К. А. Набатов, О. Г. Иванова. – М. : «Издательство Машиностроение-1», 2007. – 152 с.

А.В. Киселева, М.А. Кудрина

СТЕГАНОГРАФИЯ И МЕТОДЫ СТЕГОАНАЛИЗА

(Самарский национальный исследовательский университет
имени академика С.П. Королева)

Стеганографическая система или стегосистема – совокупность средств и методов, которые используются для формирования скрытого канала передачи информации [1]. В качестве данных может использоваться любая информация: текст, сообщение, изображение и т. п.

Контейнер – любая информация, предназначенная для сокрытия тайных сообщений.

По используемому принципу скрытия методы компьютерной стеганографии делятся на два основных класса: методы непосредственной замены и спектральные методы. Если первые, используя избыток информационной среды, заключаются в замене малозначительной части контейнера битами секретного сообщения, то другие для скрытия данных используют спектральные представления элементов среды, в которую встраиваются скрываемые данные.

В рассматриваемой системе были реализованы следующие методы стеганографии: метод замены наименьших значащих битов или LSB-метод, метод Куттера-Джордана-Боссена, метод Коха-Жао, а так же метод скрытой передачи цветных изображений bmp.

Стегоанализ – наука о выявлении факта передачи скрытой информации в анализируемом сообщении. В некоторых случаях под стегоанализом понимают также извлечение скрытой информации из содержащего её сообщения и (если это необходимо) дальнейшую её дешифровку [2].

По объекту поиска в стегоконтейнерах стегоаналитические методы можно разделить на такие типы:

1) сигнатурные методы, построенные на поиске в стеганограммах фрагментов кода, которые оставляют после своей работы стеганографические программы;
2) вероятностные методы, которые основаны на анализе вероятностных показателей, характерных для стегосообщений.

Визуальная атака на стегосистемы относится к сигнатурным методам стегоанализа. Она основана на том, что между младшими битами соседних элементов естественных контейнеров имеются существенные корреляционные связи. Также выявлены зависимости между наименее значащими и остальными битами элементов естественных контейнеров [3].

На рисунке 1 показано исходное изображение и изображение, сформированное только из наименее значащих битов (НЗБ) пикселов исходного изображения. На рисунке 2 – стегосистема и изображение, сформированное только из НЗБ пикселов стегосистемы. Различие между контейнером и стегосистемой визуально не проявляется. Но если изображение сформировать только из НЗБ пикселов стегосистемы, то можно легко увидеть следы вложения.

Атака на основе анализа статистики Хи-квадрат - вероятностный метод стегоанализа [3]. Это метод анализа закономерностей в вероятностях появления соседних номеров цвета пикселов. Номер цвета, двоичное представление которого заканчивается нулевым битом, назовем левым (L), а соседний с ним номер цвета, двоичное представление которого заканчивается единичным битом - правым (R). Пусть цветовая гамма исходного контейнера включает 8 цветов. Следовательно, при встраивании сообщения в НЗБ цветовой компоненты пикселов необходимо исследовать статистические характеристики в 4 парах номеров цвета. На рис.3 слева показана одна из типичных гистограмм вероятностей появления левых и правых номеров цвета в естественных контейнерах. Справа показана гистограмма вероятностей появления левых и правых номеров цвета в стегосистеме, сформированной из этого контейнера. Видно, что вероятности появления левых и правых номеров цвета в естественных контейнерах существенно различаются между собой во всех парах, а в стегосистеме эти вероятности выровнялись. Это является явным демаскирующим признаком наличия скрываемой информации. Заметим, что среднее значение вероятностей для каждой пары в стегосистеме не изменилось по сравнению с контейнером (показано на рис.3 пунктирной линией).

Рассмотрим алгоритм стегоанализа, базирующийся на сжатии данных. В качестве инструмента могут выступать широко распространенные программы-архиваторы [4]. Идея метода состоит в следующем: поток случайных данных сжимается хуже, чем поток, где встречаются повторяющиеся последовательности. Информация, включаемая в младшие биты контейнера, как правило, предварительно шифруется и, возможно, сжимается, поэтому является псевдослучайной. Степень сжатия контейнеров используется для определения наличия в них скрытой информации. Пусть X – последовательность, которая подается на

вход программе, а Y = ϕ(X) – новая последовательность, полученная с помощью псевдослучайного изменения младших битов всех байтов последовательности X.

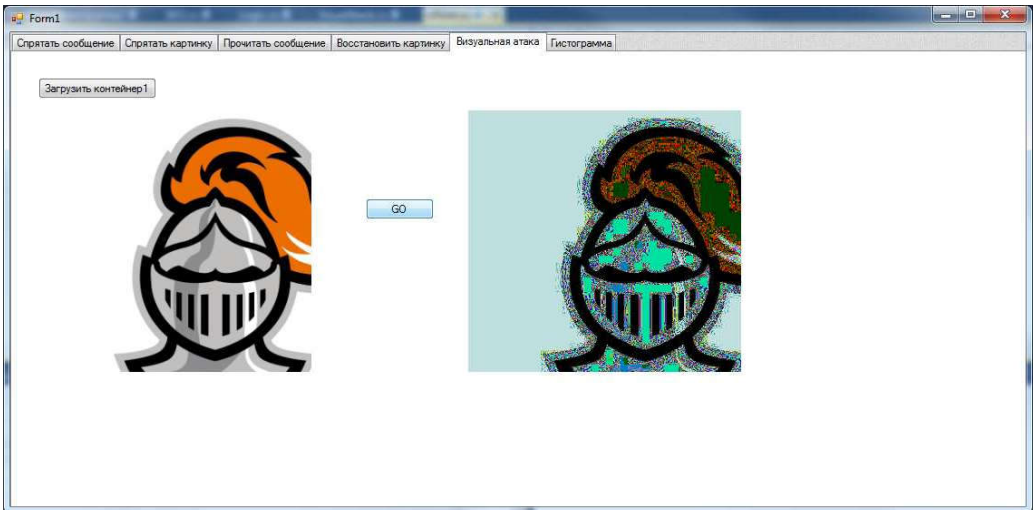

Рисунок 1 – Анализ исходного изображения

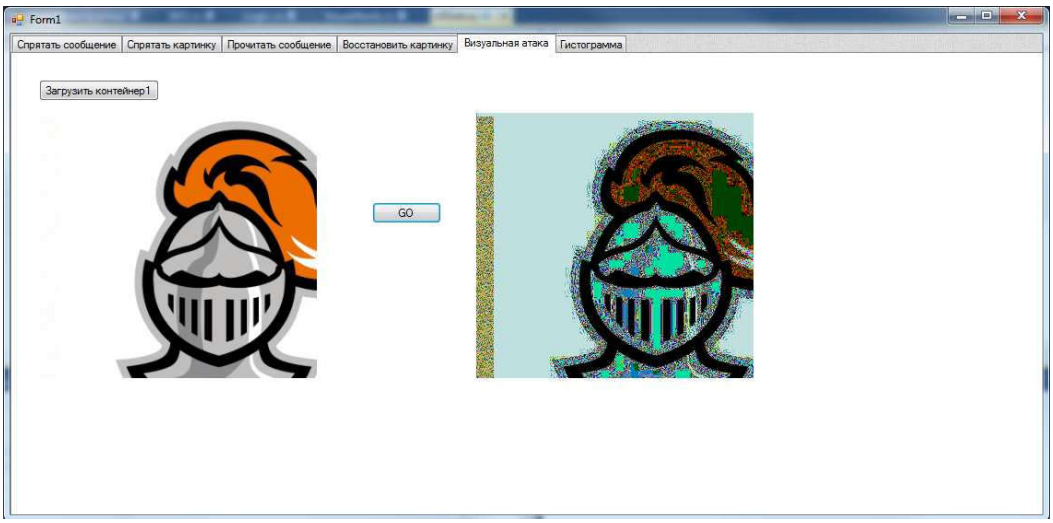

Рисунок 2 – Анализ сегосистемы

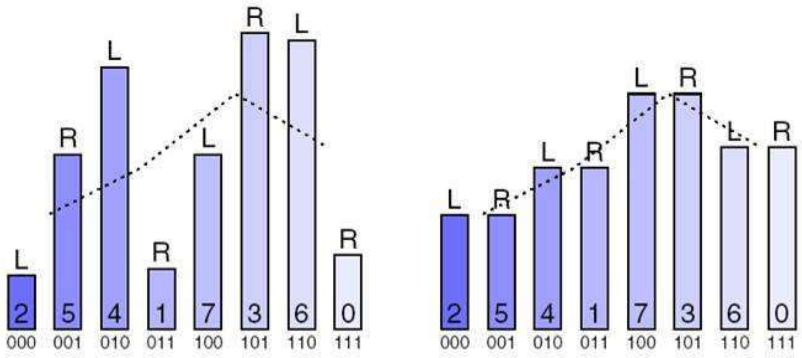

Рисунок 3 – Гистограмма частот появления левых и правых номеров цвета, слева – до встраивания, справа – после.

Отрезки последовательности X, которые не содержали «скрытую» информацию, сжимаются лучше, чем соответствующие им отрезки последовательности Y, и, напротив, коэффициенты сжатия отрезка последовательности X со «спрятанной» информацией и отвечающего ему отрезка последовательности Y отличаются незначительно. Для определения факта включения информации выбирается пороговое значение для разности коэффициентов сжатия и производится оценка количества отрезков, на которых значение этой разности не превышает порог.

В представленной работе проводится анализ стойкости методов стеганографии к приведенным методам стегоанализа. Легко видеть, что самым уязвимым методом стеганографии является LSB-метод, так как наличие встроенной информации обнаруживается любым из исследуемых методов стегоанализа. Метод Коха-Жао является самым стойким из реализованных в работе методов стеганографии, так как для встраивания информации использует частотную область контейнера и заключается в относительной замене величин коэффициентов дискретного косинусного преобразования, то есть не изменяет непосредственно младшие биты цветовых компонент контейнера.

Литература

1. Основные положения стеганографии [Электронный ресурс] - http://citforum.ru/internet/securities/stegano.shtml

2. Стегоанализ [Электронный ресурс] - https://ru.wikipedia.org/wiki/Стегоанализ

3. Практические оценки стойкости стегосистем [Электронный ресурс] - http://crypts.ru/prakticheskie-ocenki-stojkosti-stegosistem.html

4. Стегоанализ графических данных в различных форматах [Электронный ресурс] - http://old.tusur.ru/filearchive/reports-magazine/2008-2-1/63-64.pdf

М.К. Костанян, Я.В. Соловьева

АВТОМАТИЗИРОВАННАЯ СИСТЕМА ОНЛАЙН-БРОНИРОВАНИЯ НОМЕРОВ В ОТЕЛЕ

(Самарский университет)

Автоматизация взаимоотношений организаций с клиентами (CRM, сокращение от англ. *Customer Relationship Management*) применяется на современном этапе практически во всех сферах деятельности, поэтому в настоящее время автоматизация бронирования номеров в гостинице является актуальным. Основным направлением развития взаимоотношений между организациями и клиентами является разработка web-приложений для организаций.

С середины прошлого века компании во всем мире стали внедрять системы управления взаимоотношениями с клиентами в свои бизнес-процессы. Такие системы обладают самыми разнообразными возможностями: от регистра-