УДК 621.391

А.Ф. Чернявский[1], И.Л. Чваркова[2], В.С. Садов[2]

СТЕГОСТОЙКОСТЬ КЛЮЧЕВЫХ СХЕМ СТЕГАНОГРАФИЧЕСКОГО ВСТРАИВАНИЯ ИНФОРМАЦИИ

Рассматриваются вопросы повышения стойкости стеганографических систем защиты информации путем использования ключевых схем встраивания данных. Показывается, что при правильном выборе схемы встраивания и параметров стегосистемы можно существенно повысить ее стегостойкость без существенного уменьшения пропускной способности стегоканала.

Введение

Использование стеганографических алгоритмов для защиты цифровой информации становится все более популярным. В основу выбора алгоритма встраивания в большинстве случаев положены результаты анализа стойкости стеганографического канала. Одним из направлений, позволяющим повысить стегостойкость, является использование ключевой схемы при встраивании сообщения, причем различным ключевым стеганографическим схемам присущи и соответствующие степени стегостойкости. Как правило, при повышении стегостойкости пропускная способность канала уменьшается в соответствии с обратной зависимостью. Поэтому задача выбора схемы встраивания при обеспечении оптимальных значений параметров стегосистемы является нетривиальной и требует соответствующих исследований.

1. Постановка задачи

Совокупность средств и методов, которые используются с целью формирования скрытого канала передачи, образует стеганографическую систему или стегосистему [1]. Для построения теоретической модели стеганографической системы (рис.1) необходимо ввести следующие определения.

Стеганографическое поле SF – пространство стеганографического канала, его объекты, а также методы встраивания и обнаружения:

$$SF = \left(SC, C, M, K, \hat{C}, E, D\right). \tag{1}$$

Объекты стеганографического поля:

c – контейнер, $c \in C$, где C – множество всех контейнеров;

m – сообщение, $m \in M$, где M – множество всех сообщений;

k – ключ, $k \in K$, где K – множество всех ключей;

$\hat{c}$ – заполненный или модифицированный контейнер, $\hat{c} \in \hat{C}$, где C – множество всех заполненных контейнеров.

Метод встраивания E в общем случае – набор инструкций, осуществляемых над стеганографическим контейнером с учетом ключевой схемы для встраивания сообщений и получения модифицированного контейнера:

$$E : C \times M \times K \to \hat{C},\ \hat{c} = E(c, m, k), \tag{2}$$

где $c \in C$, $m \in M$, $k \in K$ и $\hat{c} \in \hat{C}$.

Метод обнаружения D в общем случае – набор инструкций, осуществляемых над модифицированным контейнером с учетом ключевой схемы для обнаружения и извлечения сообщений:

$$D : \hat{C} \times K \to M,\ m = D(\hat{c}, k), \tag{3}$$

где $m \in M$, $k \in K$ и $\hat{c} \in \hat{C}$.

Пространство стеганографического канала SC – пространственная, и/или временная, и/или частотная область мультимедийных данных, пригодная для стеганографической передачи сообщений:

$$F : C \to SC, \quad sc = F(c), \\ SC \subset C. \tag{4}$$

Стеганографическая система SS – программно-техническое средство, осуществляющее действие над объектами стеганографического поля в пределах пространства стеганографического канала посредством методов встраивания или обнаружения:

$$SS(SC, E): C \times K \times M \to \hat{C}, \ \hat{c} = SS_{SC,E}(c, k, m); \\ SS(SC, D): \hat{C} \times K \to M, \ m = SS_{SC,D}(\hat{c}, k). \tag{5}$$

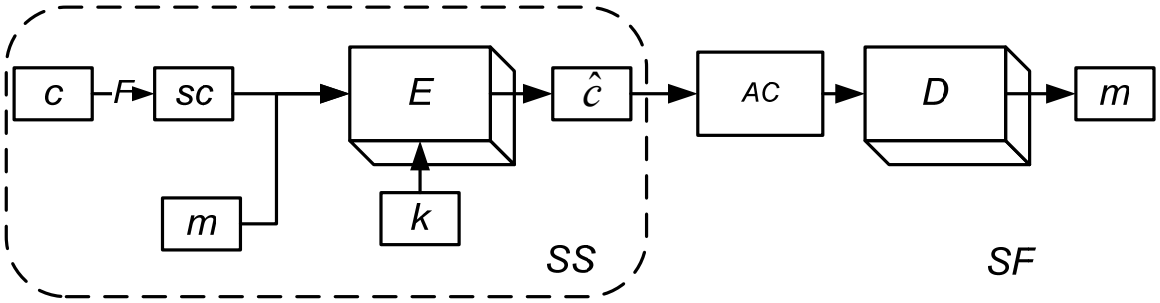


Рис. 1. Обобщенная схема стеганографической системы

Различают также следующие виды стеганографических систем SS в зависимости от типа ключа k:

– с открытым ключом $k_o \in K_o$, $k_{os} \in K_{os}$;

– с секретным ключом $k_s \in K_s$.

В системах с открытым ключом используются два ключа, независимые друг от друга. Один из ключей $k_o \in K_o$ является открытым, т. е. может передаваться свободно по незащищенному каналу связи, второй $k_{os} \in K_{os}$ является закрытым и не может быть получен посредством вычислений из ключа $k_o \in K_o$.

В стегосистеме с секретным ключом используется один секретный ключ $k_s \in K_s$, который должен быть определен либо до начала обмена секретными сообщениями, либо передан по защищенному каналу. Стеганографическая система будет осуществлять действие над объектами в соответствии с ключом.

В данной схеме блок *AC* представляет собой канал атак нарушителя. Так как целью отправителя является скрытие самого факта передачи сообщения *m*, то под стойкостью стеганографической системы подразумевается невозможность обнаружения факта информационного обмена между отправителем и получателем, а также невозможность извлечения и чтения этой информации [2].

В стеганографической системе SS (см. рис. 1) ключ k (открытый или закрытый) может участвовать в процессе встраивания сообщения, распределяя сообщение по контейнеру, либо использоваться как цифровая подпись. Таким образом, целью данной работы является исследование возможных вариантов использования секретного ключа k в стеганографической системе SS и проведение анализа влияния вида ключевой стеганографической схемы на шумовые характеристики стегофайлов, которые могут быть оценены классическими мерами, а также проведение анализа стойкости стеганографических систем с использованием статистических атак.

2. Принципы повышения защищенности стеганографических систем

Встраивание сообщения в стеганографической системе может осуществляться как по бесключевой схеме, так и с использованием ключа, что повышает стойкость стеганографического канала. Существует несколько вариантов применения ключа k в стеганографической системе *SS*: ключ может быть использован в качестве верификационного параметра, может оказывать влияние на распределение бит сообщения в пределах контейнера, а также на порядок формирования последовательности встраиваемых бит сообщения [2]. Можно выделить несколько степеней защиты стеганографического канала передачи скрываемых сообщений.

Первая степень защиты определяется выбором алгоритма встраивания (2) и базового метода модификации контейнера, реализованного в данном алгоритме. Это может быть метод замены младших значащих бит контейнера либо методы модификации частотных или пространственно-временных характеристик контейнера. Первая степень защиты присутствует в любом стеганографическом канале передачи сообщений. Стеганографическая система с первой степенью защиты (рис. 2) нашла свое применение в таком стеганографическом программном продукте, как, например, FortKnox 3.55 [3].

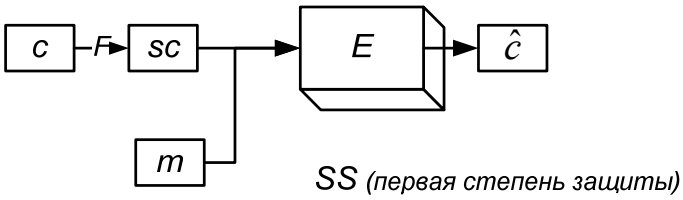


Рис. 2. Стеганографическая система с защитой первой степени

Вторая степень защиты стегосистемы, а также степени защиты более высоких порядков обеспечиваются наличием ключевых стеганографических схем. Простейшие ключевые схемы позволяют добавить лишь одну степень защиты стеганографическому каналу. Это предполагает запись немодифицированного или модифицированного пароля в начало или конец сообщения, распределение парольной подписи по всей длине стеганографического канала. Такие ключевые схемы не влияют на распределение сообщения по контейнеру и не подвергают сообщение предобработке согласно выбранному ключу (рис. 3).

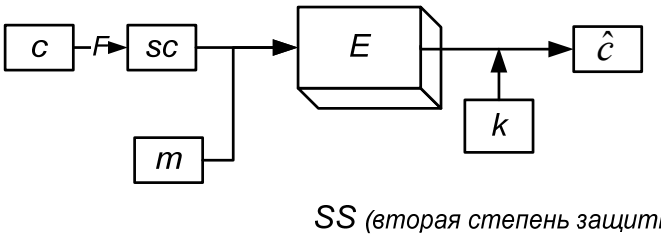


Рис. 3. Стеганографическая система с защитой второй степени

Стеганографические системы с защитой второй степени находят применение в таких задачах, как, например, добавление цифровой подписи для доказательства авторских прав. Скорость обработки контейнера при этом не изменяется. Данные системы нашли применение в следующих стеганографических программных продуктах: Data Stash [4], C1oak 7.0 [5], Steganography 1.50 [6] и Data Stealth 1.0 [5].

Наиболее защищенными являются стеганографические каналы передачи данных с ключевыми схемами встраивания информации, влияющими на способ распределения сообщения по контейнеру и/или проводящими предварительную обработку встраиваемого сообщения. Третий уровень защиты соответствует решению, когда ключ влияет на распреде-

ление сообщения по контейнеру (рис. 4, *а*). Соответственно скорость обработки контейнера будет ниже, чем в случае применения ключевой схемы первого и второго порядков. Процесс сокрытия данных в соответствии с третьей степенью защиты представляется в виде следующего алгоритма:

1. Выбор типа стеганографической системы.

Если стеганографическая система содержит открытый ключ, то первоначальным этапом является поиск соответствия между ключом $k_o \in K_o$ и $k_{os} \in K_{os}$. Ключ k_{os} будет использоваться для построения функции распределения сообщения по контейнеру. Если стеганографическая система содержит секретный ключ $k_s \in K_s$, то k_s служит для построения этой функции распределения сообщения.

2. Определение входных параметров стеганографической системы.

Входными параметрами для функции распределения сообщения по контейнеру будут являться $m \in M$, $c \in C$, $k \in K$ (открытый или закрытый).

3. Определение L – минимального количества отсчетов контейнера, необходимого для внедрения одного отсчета сообщения.

Например, для встраивания 8-битного отсчета сообщения при кодировании младших бит 8-битного аудиоконтейнера необходимо 8 байт этого контейнера. Минимальное L в общем случае определяется методом встраивания.

4. Определение P – шага распределения сообщения по контейнеру.

На основании введенного отправителем ключа встраивания k, в общем случае представляющего строку пароля (набор символов), производится определение шага распределения P сообщения m по контейнеру c. Одним из множества вариантов преобразования строки символов в число является, например, поиск соответствия в таблице кодов ASCII. В общем случае отправитель может предложить собственную таблицу соответствий печатных символов.

После нахождения соответствия каждой букве строки определенного числового кода одним из вариантов вычисления шага распределения P сообщения m по контейнеру c может быть следующий алгоритм:

1) сложение кодов ASCII всех символов строки пароля;

2) деление суммы на заданное отправителем число S_p;

3) определение P как остатка от деления суммы на число S_p.

Таким образом, отправитель преобразует ключ в число $P = P(k, S_p)$. Одним из обязательных условий возможности распределения сообщения по контейнеру в соответствии с ключом является соблюдение следующего правила:

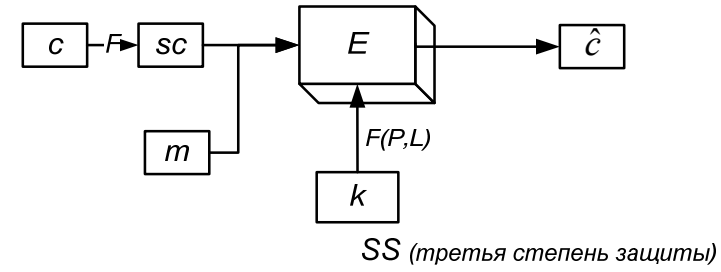
$$P \geq L. \tag{6}$$

5. Задание функции распределения сообщения по контейнеру $F(P, L)$.

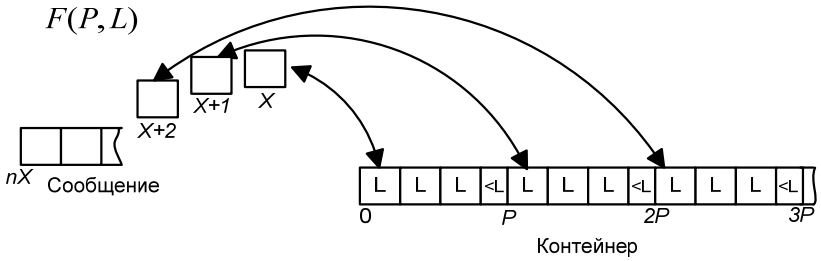
В соответствии с вычисленным шагом распределения P контейнер разбивается на блоки – своеобразные «ящики» для хранения отсчета сообщения. Размер каждого блока равен шагу *P*. Последний блок по величине может быть меньше P, если емкость контейнера не кратна P. Каждый блок контейнера содержит ряд зон встраивания емкостью *L* каждая, причем последняя зона в блоке может быть менее *L* и поэтому не подлежит встраиванию.

Одним из множества алгоритмов распределения бит сообщения по контейнеру может быть алгоритм сквозного прохода по порядку. Первый отсчет *x* сообщения заполняет первый блок контейнера от позиции 0 в первой зоне встраивания до позиции L (рис. 4, *б*), следующий отсчет $x+1$ сообщения аналогичным образом записывается во второй блок контейнера и т. д.

После заполнения сообщением всех первых зон встраивания блоков контейнера в том же порядке заполняются следующие зоны блоков контейнера, начиная опять с первого блока. Отсчеты сообщения следуют по порядку: x, $x+1$, $x+2$,…, nx.



а)



б)

Рис. 4. Стеганографическая система с защитой третьей степени:
а) обобщенная схема; *б)* детальный вид функции встраивания сообщения $F(P,L)$

Таким образом, функция распределения сообщения по контейнеру может быть представлена как

$$F(P,L) = cycle * L + step * P, \tag{7}$$

где *step* – номер шага встраивания; *cycle* – номер текущей зоны L. При таком подходе необходимо учитывать номер текущего прохода контейнера, чтобы не допустить пересечения и встраивания в уже заполненные ячейки, а также номер блока сообщения, чтобы избежать пересечений и сохранить возможность извлечения сообщения.

6. Встраивание сообщения.

Встраивание сообщения производится в соответствии с алгоритмом (2) и порядком, определенным функцией распределения $F(P,L)$. Одной из особенностей данного алгоритма является то, что если размер зоны L кратен размеру блока P, а размер блока P кратен размеру контейнера, пропускная способность такого канала не уменьшается. Происходит разупорядочение сообщения по контейнеру в соответствии с функцией распределения сообщения по контейнеру, однако все его области заполняются равномерно и не остается пустых участков.

Отличие четвертой степени защиты от третьей состоит в том, что в стегосистеме используются две функции распределения сообщения по контейнеру. Первая функция $G(Q,N)$ отвечает за порядок выбора отсчетов сообщения, а вторая функция $F(P,L)$ – за порядок выбора позиции в контейнере для встраивания отсчета сообщения. Процесс сокрытия данных в соответствии с четвертой степенью защиты представляется в виде следующего алгоритма:

1–5. Данные шаги алгоритма идентичны тем, которые использовались в стеганографической системе с защитой третьей степени.

6. Одной из множества функций выбора отсчетов сообщения может быть функция $G(Q,N)$, по сути аналогичная функции $F(P,L)$. Встраиваемое сообщение разбивается на блоки размером Q. Величина Q в соответствии с некоторой функцией преобразования $Q = Q(k, S_{\mathrm{Q}})$ вычисляется по строке символов, применяемой пользователем в качестве секретного ключа или пароля. Каждый блок Q по величине должен удовлетворять условию

$$Q \geq N, \tag{8}$$

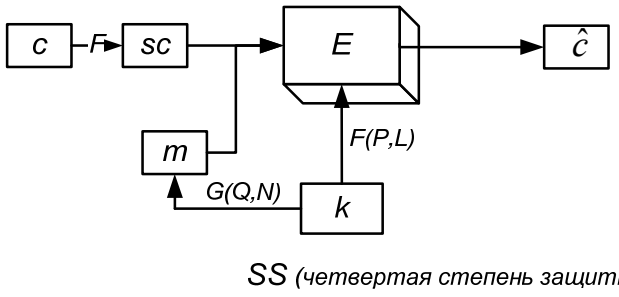
где N – размер отсчета сообщения в битах. Минимальный размер N равен 1 бит, Q всегда делится на N без остатка для того, чтобы каждый бит сообщения был встроен в контейнер.

Аналогично (7) одним из вариантов выбора бит сообщения может быть вариант, соответствующий функции $G(Q,N)$:

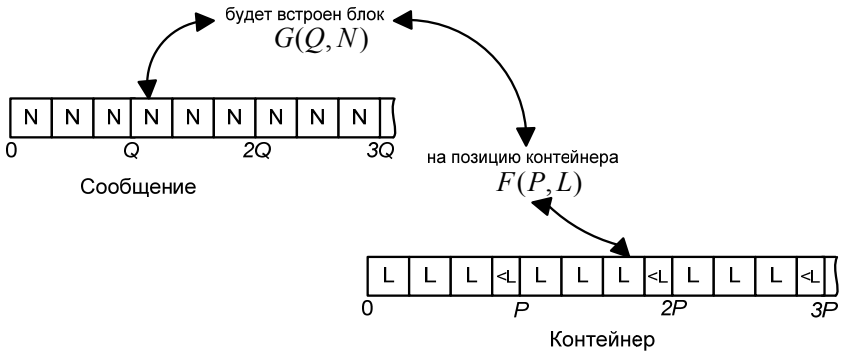
$$G(Q,N) = cycle * N + step * Q \ , \tag{9}$$

где $step$ – номер блока отсчета; $cycle$ – номер текущей области N.

7. Встраивание производится в соответствии с функциями $G(Q,N)$ и $F(P,L)$ (рис. 5).



а)



б)

Рис. 5. Стеганографическая машина с защитой четвертой степени: *а)* обобщенная схема; *б)* детальный вид функции распределения и встраивания сообщения $G(Q,N)$ и $F(P,L)$

Вышеизложенное можно свести в табл. 1.

Таблица 1

Классификационная таблица ключевых стеганографических схем

Степени защиты стеганографического канала	Наличие стеганографического алгоритма	Наличие ключей	Влияние ключей на распределение бит сообщения по контейнеру	Влияние ключей на порядок формирования последовательности встраиваемых бит сообщения
1	+	–	–	–
2	+	+	–	–
3	+	+	+	–
4	+	+	+	+

3. Количественные оценки стегостойкости для различных схем встраивания данных

Для представителей различных классов аудиоконтейнеров 8- и 16-битной кодировок и контейнеров-изображений 24-битной кодировки (8 бит на каждый растр цвета) проведено исследование, направленное на выявление зависимости количественных показателей стегостойкости системы от выбранной схемы встраивания данных.

В качестве метода встраивания E было использовано замещение младших значащих бит контейнера как наиболее распространенный метод стеганографического встраивания [2]. В качестве встраиваемых данных использовались одни и те же наборы файлов, относящиеся к различным типам: подверженные процедуре вторичного сжатия и не подверженные.

Стегостойкость канала оценивалась по классическим мерам RMS (среднеквадратическому отклонению) и PSNR (соотношению сигнал/шум). Мера RMS использовалась для оценки шума, вносимого при стеговстраивании. Мера PSNR использовалась для оценки отношения между максимальным значением сигнала-контейнера и уровнем вносимых шумовых искажений.

Оценка стегостойкости канала к статистическим атакам производилась по значениям вероятностей наличия скрываемого сообщения, полученным с применением критериев *X*-квадрат (с учетом условий, описанных в статье [7]), *X*-квадрат с поправкой [8], дельта-критерия [9], и по распределению однобитного шума изображения или наименее значащего бита (НЗБ) [10]. Результаты исследований приведены в табл. 2.

Таблица 2

Показатели обнаружения стеганографического канала при использовании различных схем встраивания данных

Ключевая схема	RMS (среднеквадратическое отклонение)	PSNR, дБ (соотношение сигнал/шум)	Вероятность обнаружения по критерию *X*-квадрат, %	Вероятность обнаружения по критерию *X*-квадрат с поправкой, %	Вероятность обнаружения по дельта-критерию, %	Вероятность обнаружения по НЗБ для изображений
1	2	3	4	5	6	7
Аудиоконтейнер (8 бит)						
Ключевая схема 1 (заполнение до 50 %)	0,49	51,14	21,11	23,22	70,54	–
Ключевая схема 2 (заполнение до 50 %)	0,49	51,14	21,11	23,22	70,54	
Ключевая схема 3						
заполнение до 20 %	0,32	52,90	0	0	54,12	
заполнение от 21 до 40 %	0,43	51,63	0	0	56,76	
заполнение от 41 до 60 %	0,54	50,52	1,68	1,97	60,67	
заполнение от 61 до 80 %	0,61	49,64	9,65	10,62	65,80	
заполнение от 81 до 100 %	0,69	49,64	19,78	20,76	69,78	
Ключевая схема 4						
заполнение до 20 %	0,32	52,90	0	0	48,71	
заполнение от 21 до 40 %	0,43	51,63	0	0	61,28	
заполнение от 41 до 60 %	0,54	50,52	0	0	62,34	
заполнение от 61 до 80 %	0,62	49,64	9,12	10,94	65,70	
заполнение от 81 до 100 %	0,69	49,64	19,67	21,64	69,79	
Аудиоконтейнер (16 бит)						
Ключевая схема 1 (заполнение до 50 %)	0,55	98,72	–	–	71,28	–
Ключевая схема 2 (заполнение до 50 %)	0,55	98,72			71,28	
Ключевая схема 3						
заполнение до 20 %	0,34	100,85			49,67	
заполнение от 21 до 40 %	0,49	99,34			54,64	
заполнение от 41 до 60 %	0,55	98,72			59,65	

Продолжение табл. 2

1	2	3	4	5	6	7
заполнение от 61 до 80 %	0,62	97,83			66,78	
заполнение от 81 до 100 %	0,68	97,83			70,67	
Ключевая схема 4						
заполнение до 20 %	0,30	101,54	–	–	48,54	–
заполнение от 21 до 40 %	0,38	100,22			53,39	
заполнение от 41 до 60 %	0,55	98,72			56,65	
заполнение от 61 до 80 %	0,62	97,83			65,56	
заполнение от 81 до 100 %	0,68	97,83			69,72	
Контейнер-изображение (24 бит)						
Ключевая схема 1 (заполнение до 50 %)	0,39	54,84	4,1	6,2		62,12
Ключевая схема 2 (заполнение до 50 %)	0,39	54,84	4,1	6,2		62,12
Ключевая схема 3						
заполнение до 20 %	0,26	56,40	0	0		30,45
заполнение от 21 до 40 %	0,41	54,28	0	0		65,78
заполнение от 41 до 60 %	0,59	52,65	0	0		70,78
заполнение от 61 до 80 %	0,73	51,63	3,2	4,4	–	71,67
заполнение от 81 до 100 %	0,78	51,14	5,1	6,4		60,23
Ключевая схема 4						
заполнение до 20 %	0,26	56,40	0	0		29,67
заполнение от 21 до 40 %	0,41	54,28	0	0		59,89
заполнение от 41 до 60 %	0,64	52,36	0	0		71,65
заполнение от 61 до 80 %	0,73	51,63	3,4	4,1		72,45
заполнение от 81 до 100 %	0,77	51,63	4,9	5,6		61,32

Как следует из табл. 2, показатели обнаружения стегоканала для первой и второй ключевых схем встраивания одинаковы, так как при кодировании использовались одни и те же встраиваемые данные. Добавление пароля в начало или конец контейнера не оказывает влияния на статистику распределения младших бит и, следовательно, значения мер равны. Преимущество от использования второй схемы по отношению к первой состоит в том, что если нарушителю будет известен алгоритм встраивания, процесс извлечения сообщения все равно будет невозможен без секретного ключа.

Использование ключевых схем встраивания более высокого порядка не оказывает влияния на меры RMS и $PSNR$, величины которых напрямую зависят от встраиваемого файла и его объема. Так, например, при замещении 20 % младших бит контейнера битами встраиваемого сообщения значения мер указывают на лучшую стегостойкость канала, чем при 100%-м замещении.

Вероятность обнаружения встраиваемых данных по критериям X-квадрат и X-квадрат с поправкой стремится к нулю при использовании ключевых схем с третьей и четвертой степенями защиты и при заполнении контейнера до 60 %. Способность обнаружения стеганографического канала при использовании всех вариантов критериев X-квадрат в случае контейнеров-изображений достаточно мала, и эти критерии способны обнаруживать наличие встраиваемых данных только в контейнерах с количеством цветов не больше 10.

В некоторых случаях с помощью оценки однобитного шума изображения представляется возможным выявить стеганографический канал передачи данных. Однако при небольшом заполнении контейнера и при использовании ключевых схем встраивания с третьей и четвертой степенями защиты скрываемые данные равномерно распределяются по контейнеру и локализовать их практически невозможно. При замещении контейнера на 100 % наблюдается обратный эффект – скрываемые данные плотно распределяются по контейнеру, отсутствует какая-либо закономерность в распределении, и если файл-сообщение подвержен процедуре вторичного сжатия, а файл-контейнер представляет собой изображение с плотным, насыщенным и разнообразным спектром, обнаружить скрываемые данные также практически невозможно.

Дельта-критерий показывает наибольшую вероятность обнаружения скрываемых данных при использовании первой и второй схем встраивания. Одной из основных особенностей этого критерия является способность обнаруживать наличие встроенных сообщений, не подверженных процедуре вторичного сжатия, и при применении 16-битных контейнеров. Обнаружительная способность дельта-критерия значительно снижается при использовании третьей и четвертой ключевых схем встраивания, а также при уменьшении объема встраиваемых данных. В случае попыток обнаружения стегоканала, организованного с помощью третьей и четвертой схем встраивания, дельта-критерий показывает равномерно распределенные по всему файлу-контейнеру всплески вероятности встраивания. Преимуществом использования четвертой ключевой схемы встраивания по сравнению с третьей является то, что если нарушителю будет известен алгоритм внедрения и секретный ключ кодирования, извлеченное сообщение будет представлять собой разупорядоченный набор бит и возможность прочтения встраиваемых данных будет стремиться к нулю.

Заключение

Стеганографическая стойкость стегосистем в значительной степени определяется схемами встраивания данных. Использование ключевых схем встраивания с разупорядочиванием областей встраивания контейнера и бит сообщения в соответствии с подобранными функциональными зависимостями позволяет значительно повысить защищенность стегоканала и при этом не снизить его пропускной способности.

Список литературы

1. Конахович, Г.Ф. Компьютерная стеганография. Теория и практика / Г.Ф. Конахович, А.Ю. Пузыренко. – Киев: МК-Пресс, 2006. – С. 288.

2. Грибунин, В.Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. – М.: СОЛОН-Пресс, 2002. – С. 272.

3. Программный продукт FortKnox [Электронный ресурс]. – Режим доступа: http://www.clickok.co.uk/steg/index.html. – Дата доступа: 11.05.2008.

4. Программный продукт Data Stash [Электронный ресурс]. – Режим доступа: http://www.skyjuicesoftware.com/software/ds_info.html. – Дата доступа: 11.05.2008.

5. Программный продукт C1oak 7.0, Data Stealth 1.0 [Электронный ресурс]. – Режим доступа: http://www.topshareware.com. – Дата доступа: 11.05.2008.

6. Программный продукт Steganography 1.50 [Электронный ресурс]. – Режим доступа: http://www.pipisoft.com/. – Дата доступа: 11.05.2008.

7. Чваркова, И.Л. Оценка применимости критерия Хи-квадрат для обнаружения стеганографического канала в аудиоданных / И.Л. Чваркова, А.Ф. Чернявский, В.С. Садов // Вестник БГУ. – 2005. – Сер. 1, № 2. – С. 92–96.

8. Чваркова, И.Л. Оценка возможности обнаружения стеганографического аудиоканала путем исследования статистики распределения соседних уровней громкости / И.Л. Чваркова, В.С. Садов // Инженерный вестник. – 2006. – № 1 (21) 3. – С. 282–289.

9. Чваркова, И.Л. Алгоритм обнаружения стеганографического канала, основанный на статистике распределения соседних уровней громкости / И.Л. Чваркова, В.С. Садов, А.Ф. Чернявский // Электроника Инфо. – 2007. – № 2. – С. 56–60.

10. Чваркова, И.Л. Обнаружение стеганографического канала передачи данных путем анализа однобитного шума изображения / И.Л. Чваркова, В.С. Садов // Известия Белорусской инженерной академии. – 2005. – № 1 (19)/2 – С. 175–178.

Поступила 17.03.08

[1]*НИИ ПФП им. Севченко БГУ,*
Минск, Курчатова, 7

[2]*Белорусский государственный университет,*
Минск, пр-т Независимости, 4
e-mail: iryna.chvarkova@googlemail.com,
sadov@bsu.by

A.F. Cherniavsky, I.L. Chvarkova, V.S. Sadov

KEY-SCHEMES STEADFASTNESS IN STAGANOGRAPHIC INFORMATION EMBEDDING

The questions of improvement staganographic steadfastness of protection information via using key schemes of embedding data are described. It was shown, that it is possible by the proper choice of coding scheme and embedding parameters to increase essentially the steadfastness without significant decreasing of staganographic channel capacity.