УДК 51-74

СТЕГАНОГРАФИЧЕСКОЕ ИСПОЛЬЗОВАНИЕ СТРУКТУРЫ СИГНАЛА ЦИФРОВОГО ИЗОБРАЖЕНИЯ

Котцов В.А., *научный сотрудник Института космических исследований Российской академии наук (ИКИ РАН), e-mail: vladkott@mail.ru;*
Котцов П.В., *инженер-программист, e-mail: kot_scorp@mail.ru.*

STEGANOGRAPHIC USE OF THE STRUCTURE OF THE SIGNAL OF THE DIGITAL IMAGE

Kotchov V.A., Kotchov P.V.

A simple steganographic method of hidden transmission of digital video information based on tabular – binary encoding is proposed. An example of the method implementation is given. Limitations and advantages in its use are noted.

Key words: steganographic method, videoinformation, hidden transmission.

Ключевые слова: стеганография, видеоинформация, криптография, скрытая передача.

Предложен простой стеганографический способ скрытой передачи цифровой видеоинформации, основанный на таблично – бинарном кодировании. Приведен пример реализации способа. Отмечены ограничения и преимущества в его использовании.

Введение

Стеганография, также как и криптография, используется человеком с тех давних времен когда он научился передавать информацию. Оба метода дополняют друг друга и нередко их используют одновременно. С появлением компьютеров и активного обмена информацией по сети, роль стеганографических способов скрытой передачи информации значительно возросла, появилась цифровая стеганография [1]. К настоящему времени предложено множество стеганографических способов для скрытой передачи информации по сети. Большая часть их использует для этого достаточно сложные схемы. Отдельное место занимает скрытая передача видеоинформации. В настоящей работе предложен простой стеганографический способ скрытой передачи цифровой видеоинформации, который использует структуру бинарного представления цифрового сигнала. Он заключается в простом таблично – бинарном преобразовании элементов самого скрывающего изображения. Рассмотренный способ не использует ключа и не требует передачи дополнительной информации. Простота реализации делает его удобным для оперативного использования.

Зачем нужна стеганография

Как только люди стали делать сообщения появилась и необходимость скрывать их. Попытки скрыть факт передачи информации имеют длинную историю. Известны хрестоматийные примеры, когда дощечку с сообщением покрывали воском, на котором писали что-либо несущественное или, например, всем известное из детективной литературы применение «невидимых» чернил. Способы сокрытия самого факта передачи информации получили название стеганографических. Само передаваемое сообщение тоже стали шифровать. Этот способ сокрытия информации шифрованием называют криптографическими. Оба эти способа скрытой передачи конфиденциальной информации нередко дополняют друг друга. Сегодня активно развивается математическая криптография, изучающая эффективные математические модели для криптографических схем. В стеганографии также разработаны различные схемы сокрытия.

Стеганография, в буквальном смысле означает «тайнопись». Как один из методов защиты информации, она может использоваться в различных областях. Появление компьютерных систем, развитие интернета и широкое применение компьютерных технологий привели к появлению также методов цифровой стеганографии для обеспечения скрытой передачи и защиты передаваемых данных. Это относительно молодое направление, которое возникло с широким внедрением новых цифровых информационных технологий. С их быстрым распространением появилась необходимость осуществлять подтверждение значимой информации, закреплять авторство, пересылать конфиденциальные сообщения. Стеганография может выступать в роли защитника ценной информации, в целях сокрытия данных от возможного саботажа, кражи данных или нежелательного просмотра их третьими лицами. В современных компьютерных документах появились также цифровые водяные знаки, цифровая подпись и другие стеганографические приемы авторизации информации [2].

Суть стеганографических технологий заключается в том, что передаваемую конфиденциальную видеоинформацию маскируют другой информацией, например, другим изображением. Выбор маскирующего изображения имеет определенные трудности, а его регулярно повторяющаяся передача уже сама будет служить демаскирующим фактором. Многие стенографические способы передачи информации используют схему с ключом. Однако, для этого необходимо дополнительно передавать информацию о самом ключе и, если он меня-

ется, оперативно менять его при приеме очередного пакета данных.

Известные технологии способов скрытой передачи информации

Задачу встраивания и выделения сообщений из принятой информации выполняет стеганосистема. Общая схема функционирования такой стенографической системы передачи показана на рис. 1. Изображение, в которое встраивается скрываемое сообщение, называют контейнером. Операцию встраивания выполняет стеганокодер. Для преобразования скрываемого сообщения к виду удобному для встраивания в контейнер иногда может использоваться прекодер. Изображение – контейнер со встроенным сообщением передают по каналу связи. При приеме информации получателем стеганодекодер выделяет скрываемое сообщение. Для преобразования скрываемого сообщения к виду, удобному для восприятия может также использоваться посткодер.

Следует отметить, что в нашей схеме не показан ключ, который часто применяется в стеганосистемах. Но, в рассматриваемом нами способе ключ не используется, что упрощает технологию, так как исключает дополнительную проблему его передачи.

Известно множество способов скрытой передачи видеоинформации, которые относятся к стеганографии. Большинство этих способов основано на внесении небольших изменений в структуру передаваемой информации. При выборе способа для пользователя важны, как эффективность, так и оперативность выполнения процедур кодирования и декодирования видеоинформации.

При встраивании конфиденциальной видеоинформации в состав другого изображения необходимо, чтобы эта скрываемая информация не влияла на качество графики открыто передаваемого изображения - контейнера. В связи с этим изменения в структуре этого изображения – контейнера должны быть очень незначительными. Общий принцип таких методов заключается в замене избыточной, малозначимой части изображения битами скрываемого сообщения. Для извлечения этого сообщения получателю необходимо знать алгоритм, с помощью которого скрытая информация размещалась в контейнере. Тогда обратное преобразование позволит получателю его прочитать.

Известно множество различных способов скрытой передачи видеоинформации, которые относятся к области стеганографии. Многие из них подробно описаны в литературе, например, в [3].

Распространены способы, при которых передаваемую информацию модулируют некоторой известной, например, случайной зависимостью и зная эту зависимость при приеме восстанавливают информацию. Их основным недостатком является сложность синхронизации процессов кодирования и декодирования.

В частности, предложен способ секретной передачи информации при котором используют формирование исходного хаотического детерминированного сигнала генератором хаоса и модуляции параметров хаотического сигнала полезным [4].

Предложен способ скрытой передачи информации, содержащей полезный цифровой сигнал, который заключается в том, что этот полезный сигнал кодируют в двоичный код, формируют посредством первого хаотического генератора исходный детерминированный хаотический сигнал путем модуляции параметров хаотического сигнала полезным цифровым сигналом, а затем суммируют сформированный таким образом сигнал с шумовым сигналом, производимым генератором шума [5].

Предложен также способ защищенной передачи информации, включающий формирование информационного сигнала с закодированной информацией, аддитивное суммирование информационного сигнала с хаотическим маскирующим сигналом, передачу суммарного сигнала по каналу связи. Согласно этому решению в качестве информационного и маскирующего сигналов используют последовательности одиночных импульсов подобной формы, при этом кодирование информации осуществляют изменением расстояния между соседними импульсами информационного сигнала. Распознавание формы импульсов выполняют с использованием принципов нейросетевого распознавания [6].

Предложен способ засекречивания сигналов, заключающийся в том, что исходный сигнал подвергают дискретизации, причем каждый дискретный отсчет сигнала умножают на импульсную характеристику, которую формируют из импульсных характеристик отдельных частотных полос в виде последовательности временных отсчетов [7].

Существенным недостатком всех этих способов является также то, что они имеют достаточно сложную технологию реализации.

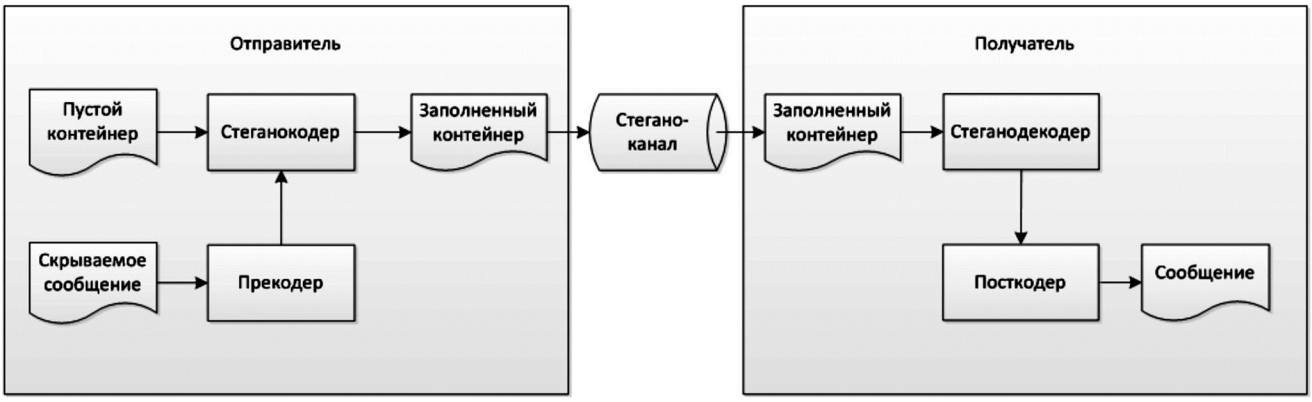


Рис. 1

Предложен достаточно простой способ кодирования и декодирования видеосигнала, при котором передают выбранную группу строк изображения в заданном порядке, который отличается от последовательного, соответствующего правильной развертке изображения [8]. Однако, при этом необходимо передавать и саму последовательность выбора для восстановления принятой информации.

Широко используют также способы сокрытия данных в пространственной области передаваемой информации. При этом различными операциями встраивают скрываемые данные в области первичного изображения-контейнера. Их преимущество заключается в том, что в большинстве случаев для встраивания скрываемой информации нет необходимости выполнять сложные и длительные преобразования изображений. Общий принцип этих методов заключается в замене избыточной, малозначимой части цифрового изображения битами скрываемого сообщения. Используемые разряды цифровых данных содержат незначительную часть полезной информации. Внесение в них дополнительной информации практически не влияет на качество восприятия. Для извлечения скрытого сообщения необходимо знать алгоритм, по которому размещалась в контейнер эта информация [9].

Среди методов замены в пространственной области наиболее широко распространен метод замены наименее значащего бита (Least Significant Bit). Младший значащий бит изображения несет в себе меньше всего информации. Специалистам известно, что человек в большинстве случаев не способен заметить изменений в этом бите. Фактически это шум, поэтому его можно использовать для встраивания информации путем замены менее значащих битов пикселей изображения битами секретного сообщения. При этом, для изображения в градациях серого объем встроенных данных может составлять существенную часть от общего объема контейнера. Однако, локализация скрытой информации на одном битовом уровне имеет свои очевидные недостатки. Если же модифицировать два младших бита (что также практически незаметно), то данную пропускную способность можно увеличить еще вдвое. Популярность данного метода обусловлена его простотой и тем, что он позволяет скрывать в относительно небольших файлах достаточно большие объемы информации. Подобный метод сокрытия информации с использованием младших бит элементов цифровых изображений подробно описан, например, в [10]. Недостатком метода является определенная сложность технологии кодирования и декодирования.

Применяется также метод случайного интервала, заключается в случайном распределении битов секретного сообщения по контейнеру, в результате чего расстояние между двумя встроенными битами определяется псевдослучайно. Этот метод особенно эффективен в случае, когда битовая длина секретного сообщения существенно меньше количества пикселей изображения. Недостатком этого метода является то, что биты сообщения в контейнере размещены в той же последовательности, что и в самом сообщении, и только интервал между ними изменяется псевдослучайно. Поэтому для контейнеров фиксированного размера более целесообразным является его усиление, путем использования псевдослучайной перестановки. Однако, все это только увеличивает сложность метода.

К методам сокрытия в пространственной области также относится метод квантования изображения, основанный на межпиксельной зависимости, которую можно описать некоторой функцией. В простейшем случае вычисляют разницу между смежными пикселями и задают ее как параметр этой функции. При данном методе скрытие информации производится путем корректировки разностного сигнала. При кодировании соответствующим образом изменяют значения интенсивностей пикселей формируемого изображения. Недостатком этого метода является необходимость использования стеганоключа, который представляет собой таблицу, где каждому возможному значению разности ставится в соответствие определенный бит.

Технология сокрытия данных в пространственной области в большинстве случаев довольно сложна. Она подробно описана в разных источниках, например, в [3].

Информационные возможности скрытой передачи видеоинформации

Рассматриваемые компьютерные технологии передачи видеоинформации используют цифровое изображение, создаваемое современными электронными средствами наблюдения. Оптический сигнал изображения воспринимается матричным фотоприемником, а величину сигнала формирует аналого-цифровой преобразователь. Таким образом получаемое в современных системах изображение всегда является дискретизованным и квантованным отображением наблюдаемой сцены.

Для каждого элемента дискретизации (пикселя) такое отображение можно представить набором единичных значений, последовательно размещенных на уровнях квантования соответственно величине яркости наблюдаемого участка. Остальные уровни этого элемента пустые, заполнены соответственно нулями. Очевидно, что при таком подходе информационное содержание каждого пикселя квантованного изображения определяется числом этих единиц, а количество нулей не несет никакой информации.

Рассмотрим следующую возможность. Перемешаем единицы и нули на разных уровнях одного пиксела между собой случайным образом. При этом можно рассматривать полученную комбинацию, как бинарный код некоторого числа. Такую информацию можно будет передать по каналу связи. При приеме эта информация может быть также представлена в бинарной форме, а после сортировки единиц и отбрасывания нулей, последовательность принятых единиц снова восстановит исходное значение амплитуды сигнала.

Такая технологическая схема преобразований сигнала позволяет производить некую скрытую передачу конфиденциальной информации. Рассмотрим основные особенности такой передачи, которые определяют ее потенциальные возможности.

Если рассмотреть множество неповторяющихся зна-

чений, на которые в ходе описанного преобразования отображается каждое из значений исходного сообщения, то можно сказать, что мощности этих множеств различны для каждого из значений исходного сообщения и определяются, как число сочетаний C_N^m, по известной формуле:

$$C_N^m = \frac{N!}{m!(N-m)!}$$

где N – значение символа исходного алфавита, соответствует числу единиц в своем бинарном представлении после преобразования, m – разрядность используемого изображения – контейнера.

Рассмотрим конкретный случай. Для определенности рассмотрим изображение, квантованное на 9 уровней. Для этого случая (m = 8), тогда мощности множеств, на которые отобразятся соответствующие исходные значения, распределятся следующим образом:

N	0	1	2	3	4	5	6	7	8
C_N^m	1	8	28	56	70	56	28	8	1

Из приведенной таблицы очевидно, что предложенное преобразование имеет наибольшую эффективность сокрытия в середине диапазона математически допустимых значений передаваемого сообщения (N), утрачивая её к границам диапазона. Это накладывает дополнительные ограничения на передаваемое секретное сообщение и его вид, пригодный для встраивания в изображение – контейнер с рассмотренными характеристиками.

Приведенный пример явно показывает, что диапазоны допустимых значений контейнера (D) и сообщения (N) связаны между собой, как $D = 2^N - 1$. Например, если в качестве контейнера используется маскирующее изображение с разрядностью 8 бит на элемент или 256 уровней со значениями 0 – 255, то в этом случае, для эффективного кодирования скрываемое сообщение может иметь не более 9 уровней.

Предлагаемый способ скрытой передачи информации

Учитывая рассмотренные выше свойства квантованного изображения, мы предложили стеганографический способ скрытой передачи видеоинформации, при котором передаваемая видеоинформация также маскируется другим заранее выбранным изображением, как это принято в стеганографиии. В этом способе, также как в многих известных, вносятся неразличимые для глаза искажения в изображение-контейнер. Однако, для его реализации используется иной подход к способу кодирования скрываемого сообщения. Основу используемого преобразования составляет таблица с алфавитом бинарного кода для представления элементов – пикселей исходного изображения – контейнера в соответствии с встраиваемой информацией – сообщением.

Предлагаемый способ осуществляется следующим образом. Для преобразования значений сигнала элементов информации-контейнера предварительно формируют эту кодирующую таблицу. В кодирующей таблице для каждого из возможных значений величины сигнала контейнера определяют число единиц в его бинарном представлении. При этом эти значения величины сигнала группируют по числу единиц в его бинарном представлении и упорядочивают эти группы по возрастанию значений числа единиц в диапазоне допустимых значений величины сигнала элементов передаваемого изображения – сообщения. Однако, для этого процесса может быть использована и другая эквивалентная методика.

Полученная кодирующая таблица для соответствующего числа уровней квантования составляется только один раз, а затем может многократно использоваться для передачи изображений. Следовательно, для оперативной передачи секретного сообщения целесообразно хранить такую кодирующую таблицу в памяти устройства.

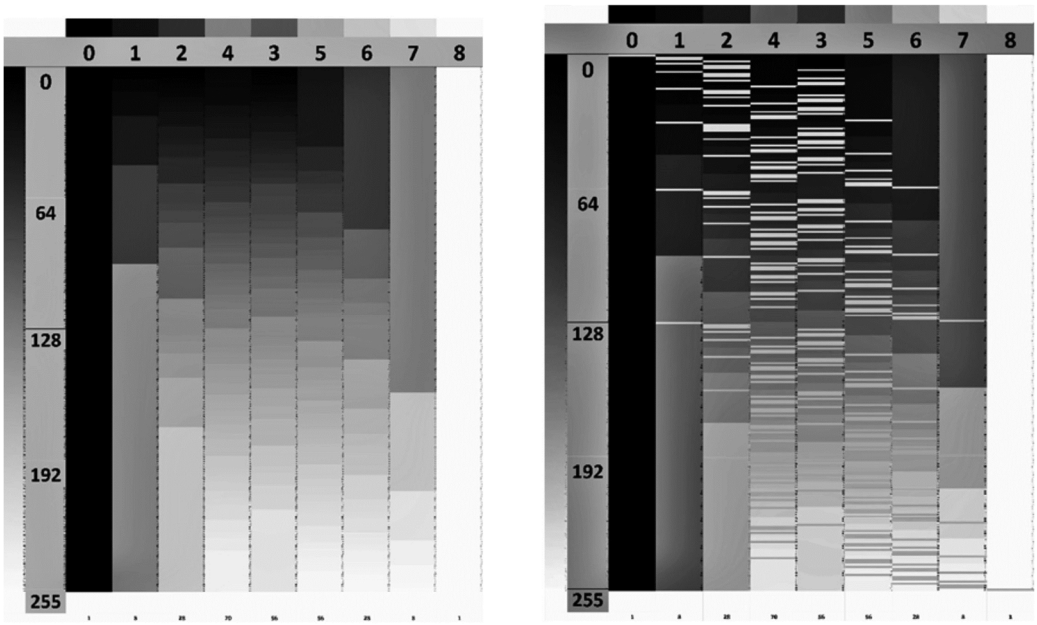
После составления этой таблицы, на этапе кодирования видеоинформации, одновременно поэлементно просматривают информацию – контейнер и информацию –сообщение и для каждого элемента сообщения по величине его значения сигнала выбирают соответствующую по порядку группу из нашей кодирующей таблицы, а после этого для каждого элемента информации – контейнера по величине его сигнала выбирают из таблицы в этой группе соответствующее ему значение и заменяют этим значением сигнала текущее значение элемента изображения – контейнера. Полученную таким образом преобразованную цифровую информацию – контейнер со встроенным сообщением передают по каналу связи.

На рис. 2 *а* показан пример кодирующей таблицы для случая использования контейнера с 256 уровней серого (по вертикали) для передачи скрытого изображения – сообщения с 9 уровнями серого (по горизонтали). На рис. 2 *б* на той же таблице выделены допустимые для использования значения, которые соответствуют поставленным условиям.

Таким образом, в предлагаемом способе значение яркости передаваемого изображения - контейнера для каждого пикселя является ближайшим приближением к значению яркости элемента незагруженного изображения - контейнера, но таким, что количество единиц в его двоичном представлении определяет соответствующее значение сигнала для передаваемого сообщения.

После приема такой видеоинформации адресатом, её вновь поэлементно просматривают и преобразуют полученное значение величины сигнала каждого элемента (пикселя) к его бинарному представлению. В бинарном представлении сигнала в виде последовательности значений 0 и 1 для каждого пикселя полученной видеоинформации, определяют количество единичных значений в ее бинарной форме или, в зависимости от выбранного варианта реализации дальнейшего представления, сортируют единицы и нули в бинарном коде для получения непрерывной последовательности единиц. Затем, на основании полученного результата формируют величину яркости сигнала переданной информации – сообщения.

В качестве примера реализации этих процедур покажем результаты программного моделирования предлагаемого способа.



а) *б)*

Рис. 2

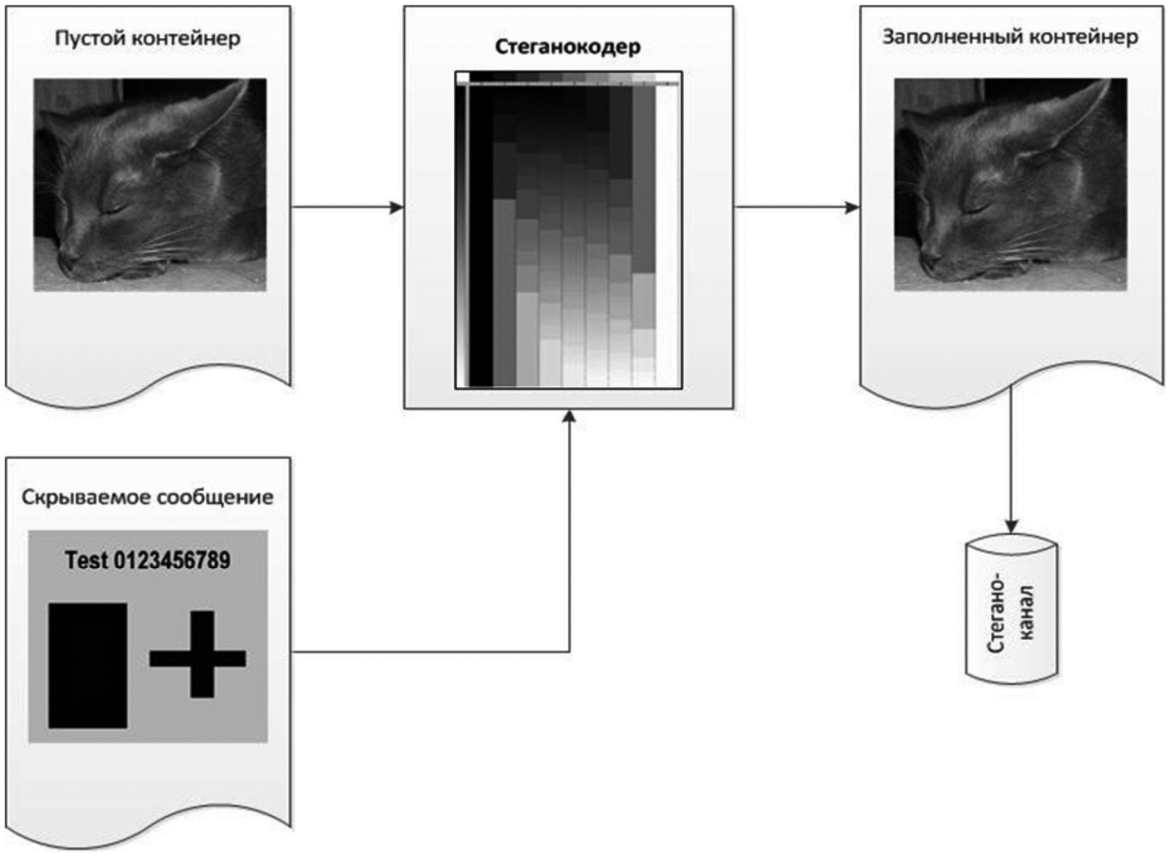


Рис. 3

На рис. 3 показана блок – схема кодирования скрываемой информации, использованная в эксперименте.

Кодированное сообщение в нашем случае передают по каналу связи без дополнительных указаний о способе кодирования. Прямое отображение переданного сообщения даст отображение изображения – контейнера. Подсчет единичных бит его бинарного представления даст отображение передаваемой информации.

Операция декодирования может быть выполнена разными способами.

Опыт показал, что эффективной операцией при определении величины сигнала скрываемой информации может быть сортировка размещения единиц и нулей по уровням квантования. Эта операция приводит на выходе к необходимому значению амплитуды сигнала. Для сортировки единичных бит в бинарном представлении

сигнала могут использоваться любые известные способы, в частности, широко применяемый в компьютерных программах метод пузырька (Bubble sort), например. Известны также аппаратные решения этой задачи [11]. Однако, более эффективен метод логической сортировки, который может выполняться в потоковом режиме. Для реализации этой операции сортировки данных может быть применена схема стеганодекодера, построенная на сдвоенных логических элементах И и ИЛИ. Она показана на рис. 4, где белым цветом показаны элементы И, а черным элементы ИЛИ. Подобная схема использовалась нами ранее для увеличения динамического диапазона изображения. Подробное описание её функционирования дано в статье [12].

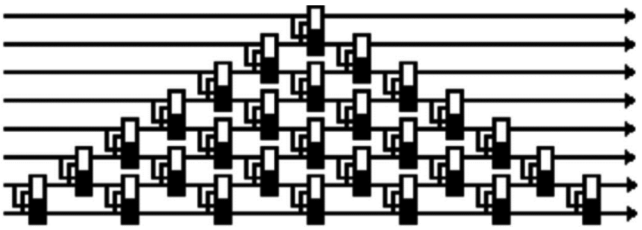


Рис. 4

На рис. 5 показана блок-схема декодирования скрываемой информации, со стеганодекодером на логических элементах И и ИЛИ, которая использовалась в нашем эксперименте.

На рис 6 показаны: а – вариант тестового изображения для скрытой передачи, б – вариант загруженного изображения – контейнера с этим тестовым изображением в нашем эксперименте. Видно, что на загруженном изображении – контейнере следов тестового изображения не наблюдается. Аналогичные результаты были получены на других тестовых изображениях.

Предлагаемый стеганографический способ скрытой передачи видеоинформации обсуждался на конференции по техническому зрению ТЗСУ-2016 [13]. На технологию описанного способа скрытой передачи видеоинформации получен патент [14], который был отмечен медалью на XXI Московском международном Салоне изобретений и инновационных технологий «Архимед-2018».

Заключение

Таким образом, передаваемое скрытое изображение является результатом простого бинарно - табличного преобразования элементов самого исходного изображения с ограничивающими факторами, которые зависят от амплитуды сигнала в каждой точке изображения - контейнера. Исходя из описания операций предложенного способа кодирования, для извлечения скрытого сообщения из контейнера, необходимо и достаточно для каждого элемента выполнить подсчет количества единичных битов в двоичном представлении значения соответствующего элемента изображения заполненного контейнера. Принимаемую видеоинформацию можно также восстанавливать путем преобразования закодированного сигнала методами сортировки. Эти процедуры автономны, просты и не требует наличия ключей или синхронизации процессов приемо-передачи. В результате описанных действий передаваемая видеоинформация может быть восстановлена оперативно и полностью, без информационных потерь. Также важно, что кодированное сообщение передают по каналу связи без дополнительных условий для декодирования.

Рассматриваемые процедуры не требуют для их осуществления сложных алгоритмов и могут быть легко реализованы на основе ПЛМ. [15] Такая реализация

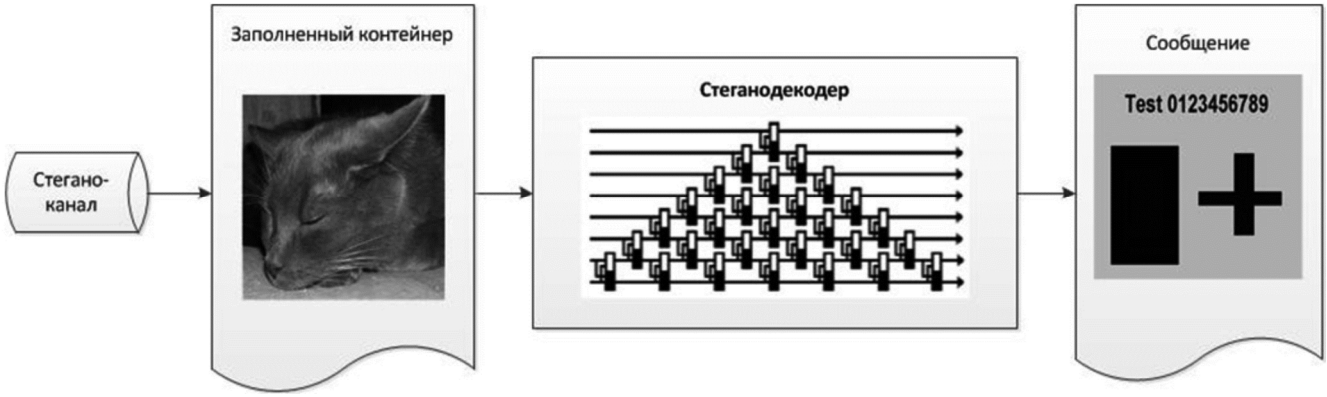
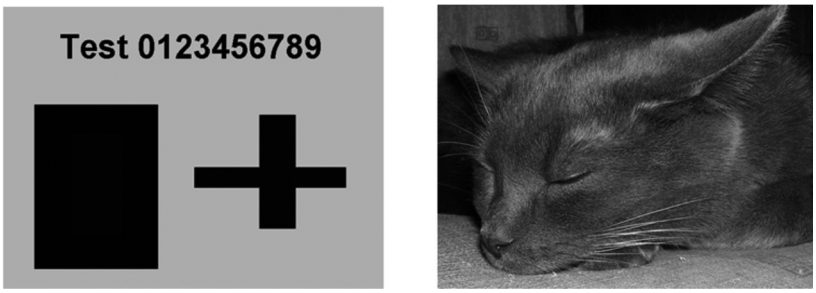


Рис. 5



а) *б)*

Рис. 6

обеспечивает потоковое декодирование, осуществляемое в темпе поступления видеоинформации.

Предлагаемую технологию стеганографического кодирования можно использовать при передаче оперативной информации ограниченного доступа, при обмене конфиденциальной документации, в платежных системах нижнего уровня, для введения цифровой подписи, для создания цифровых водяных знаков и меток для защиты авторских прав произведений, для оперативного скрытого согласования организационных мероприятий по картам и снимкам местности, в защищенных программах управления техникой и других областях, использующих технологии скрытой передачи информации.

Литература

1. Генне О.В. Основные положения стеганографии // Защита информации Конфидент. N 3, 2000.

2. Аграновский А.В., Балакин А.В., Грибунин В.Г., Сапожников С.А. Стеганография, цифровые водяные знаки и стеганоанализ. М.: Вузовская книга, 2009.

3. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. К.: МК-Пресс, 2006.

4. Короновский А.А., Москаленко О.И., Попов П.В. и др. Способ секретной передачи информации. Патент РФ 2295835// Бюллетень изобретений № 8, 2007.

5. Москаленко О.И, Короновский А.А., Храмов А.Е. Способ скрытой передачи информации с изменяющимися характеристиками генератора шума. Патент РФ 2421923// Бюллетень изобретений №17, 2010.

6. Назимов А.И., Павлов А.Н. Способ защищенной передачи информации с использованием импульсного кодирования. Патент РФ 2493659 // Бюллетень изобретений № 26, 2013.

7. Лобов Н.Н. Способ засекречивания сигналов и устройство для его осуществления. Патент РФ 2207733 // Бюллетень изобретений №08, 2005.

8. Кудельски А. Способ кодирования и декодирования видеосигнала. Патент РФ 2132114 // Заявка PCT WO 91/13517, 1999.

9. Грибунин В.Н., Оков И.Н., Туринцев И.В. Цифровая стеганография. М.: Солон-пресс, 2009.

10. Кустов В.Н., Федчук А.А. Методы встраивания скрытых сообщений // Защита информации. Конфидент. № 3, 2000.

11. Ядыкин И.М. Устройство для определения количества единиц в упорядоченном двоичном числе. Патент РФ 2522875// Бюллетень изобретений № 20, 2014.

12. Котцов В.А. Увеличение динамического диапазона видеосистемы логическим сложением цифровых изображений // Цифровая обработка сигналов №3, 2019.

13. Котцов П.В., Котцов В.А. Простой способ скрытой передачи видеоинформации // Седьмая научно-техническая конференция «Техническое зрение в системах управления – 2016», Москва 15-17 марта, 2016.

14. Котцов В.А., Котцов П.В. Способ скрытой передачи цифровой информации. Патент РФ 2636690 // Бюллетень изобретений № 33, 2017.

15. Стешенко В.Б. Плис фирмы ALTERA: проектирование устройств обработки сигналов. М. Додека, 2000.