ISSN 2658-5014 (Print) СИИТ ISSN 2686-7044 (Online)
2023. Т. 5, № 3 (12). С. 114–135 http://siit.ugatu.su
СИСТЕМНАЯ ИНЖЕНЕРИЯ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

УДК 004.65 DOI 10.54708/2658-5014-SIIT-2023-no3-p114

Инвариантные системы стеганографической защиты информации в реальном времени с использованием двухкомпонентных контейнеров

М. В. Шакурский • М. Ю. Шамшаев

Аннотация. В статье представлен обзор результатов исследования инвариантных систем стеганографической защиты информации в реальном времени. Объектом исследования являются системы защиты информации, использующие стеганографические технологии. Предмет исследования — двухкомпонентные системы стеганографической защиты информации, обеспечивающие инвариантность алгоритмов извлечения сообщения от маскирующего сигнала и обладающие высокой чувствительностью к вариации ключевых коэффициентов алгоритма. Цель — повышение эффективности стеганографической защиты информации за счёт использования двухкомпонентных контейнеров, построенных на основе преобразования двух сигналов и использования функций извлечения сообщений в области разрыва. Для достижения цели разработаны: 1) научно-практическая концепция инвариантной стеганографической системы; 2) методология реализации двухкомпонентного стеганографического контейнера; 3) способ встраивания двухкомпонентного контейнера в покрывающий объект; 4) комплекс математических моделей подсистем встраивания сигнала сообщения в двухкомпонентный контейнер и подсистем извлечения сигнала сообщения из двухкомпонентного контейнера; 5) способы выбора параметров двухкомпонентных стеганографических алгоритмов, обеспечивающих высокий уровень сокрытия информации и стойкости к взлому; 6) технические решения двухкомпонентных стеганографических систем на основе результатов численного и имитационного моделирования и программного обеспечения предложенных двухкомпонентных стеганографических систем защиты информации. Использованы методы математического и численного моделирования, системный анализ, теория чувствительности динамических систем, метод спектрального анализа, статистические методы, цифровая обработка сигналов.

Ключевые слова: стеганография; система реального времени; двухкомпонентный контейнер.

Введение

Глобальная информатизация общества и интенсивный информационный обмен требуют развития систем телекоммуникаций, проводных и беспроводных средств передачи данных. Телекоммуникационные системы в соответствии с ГОСТ Р ИСО/МЭК 27002-2021 (ГОСТ Р ИСО/МЭК 27002-2012) должны обеспечивать требования информационной безопасности, включающие в себя конфиденциальность, целостность и доступность информации. Для решения задачи защиты информации от прочтения злоумышленником используется криптографическое кодирование (ГОСТ Р 34.12–2015), обладающее высокой стойкостью к криптоанализу. Однако при использовании открытых каналов злоумышленник может разрушить кодированные сообщения или канал связи. В этом случае защиту информации способны обеспечить стеганографические методы, позволяющее осуществить скрытную передачу важной информации по открытому каналу связи так, чтобы злоумышленник не зафиксировал факт передачи и не разрушил сообщение [1, 2]. Необходимость использования стеганографии также возникает, если применение криптографических методов запрещено (на государственном или корпоративном уровне) или неэффективно. Таким образом, стеганография является эффективной защитой при передаче информации, используемой в реальном времени, а также при внедрении цифровых водяных знаков, при скрытой передаче сигналов управления, для скрытого хранения информации и в других случаях. Сказанное выше подчёркивает актуальность исследований стеганографии.

Актуальность исследования стеганографии также подтверждается и «Приоритетными направлениями развития науки, техники и технологий Российской Федерации», утвержденными Указом Президента РФ от 16 декабря 2015 г. № 623, в направлении «Безопасность и противодействие терроризму».

На сегодняшний день применение стеганографии носит не нормированный характер из-за отсутствия стандартов на её использование. Это объясняется разнообразием стеганографических алгоритмов и сложностью их классификации и стегоанализа.

Развитие цифровой стеганографии требует формирования теоретической базы и создания устойчивых методов встраивания скрываемой информации в покрывающий сигнал. Это, в перспективе, позволит прийти к стандартизации стеганографических методов.

Степень разработанности темы и обсуждение решаемой задачи

Степень проработанности данной темы характеризуется проведённым анализом существующих стегоконтейнеров, файловых систем, файлов различных форматов (текстовых, звуковых, видео, изображений), стандартов передачи данных, а также накопленной базой стеганографических алгоритмов.

Стеганографии посвящены исследования таких учёных, как R. J. Anderson, W. Bender, C. Cachin, S. Craver, J. Fridrich, N. F. Johnson, N. Morimoto, B. Pfitzmann, I. Pitas, B. Schneier, G. J. Simmons, S. Voloshynovskiy. Среди отечественных учёных следует выделить таких авторов, как С. В. Белим, И. С. Вершинин, В. Г. Грибунин, Г. Ф. Конахович, В. И. Коржик, И. Н. Оков, А. Ю. Пузыренко, В. А. Райхлин, Б. Я. Рябко, И. В. Туринцев, В. Н. Кустов, А. Н. Фионов, Л. К. Бабенко, В. В. Нечта и др.

Обзор работ показал, что все известные на сегодняшний день стеганографические алгоритмы являются однокомпонентными, то есть в сигнал контейнера подмешивается скрываемый сигнал, и формируется одна компонента. Недостатками указанных алгоритмов являются сложность извлечения скрытого сообщения, связанная с необходимостью знания принимающей стороной определённой информации о сигнале контейнера (информированный декодер), низкая устойчивости при известном алгоритме (целенаправленная атака) [3].

Работа стеганографических систем в реальном времени имеет ряд ограничений на применение современных методов, так как не позволяет анализировать или синтезировать покрывающий объект во всём его объёме. Таким образом, встраивание сообщений в реальном времени является слабо защищённым. Повышение защищённости стеганографических систем, работающих в реальном времени достигается использованием инвариантных двухкомпонентных стеганографических контейнеров. Создание таких систем является актуальной научной и технической задачей.

В данном исследовании предлагается принципиально новый подход к формированию стеганографических систем, заключающийся в формировании двухкомпонентного стеганографического контейнера, компоненты которого формируются из сигнала контейнера и двух скрываемых сигналов, связанных со входным сигналом [4–9]. Предложенный подход обладает целым рядом преимуществ:

- широкий круг алгоритмов встраивания сообщения в контейнер;
- инвариантность функций извлечения сообщения от сигнала контейнера;
- работа в области разрыва функции извлечения сообщения, обеспечивающая высокую чувствительность к ошибке, вносимой в ключевые коэффициенты алгоритма;
- работа двухкомпонентных стеганографических систем в реальном времени;
- увеличенная пропускная способность при маскировке сообщения случайным сигналом;
- возможность модификации однокомпонентных стеганографических алгоритмов в двухкомпонентные алгоритмы;
- возможность использования известных телекоммуникационных систем для передачи скрытой информации.

Таким образом, объектом данного исследования являются системы защиты информации, использующие стеганографические технологии. Предметом исследования являются двухкомпонентные системы стеганографической защиты информации, обеспечивающие инвариантность алгоритмов извлечения сообщения от маскирующего сигнала и обладающие высокой чувствительностью к вариации ключевых коэффициентов алгоритма. Цель – повышение эффективности стеганографической защиты информации за счёт использования двухкомпонентных контейнеров, построенных на основе преобразований двух сигналов, и использования функций извлечения сообщений в области разрыва.

В соответствии с этим были поставлены и решены следующие задачи:

1) Разработка научно-практической концепции инвариантной стеганографической системы.

2) Разработка методологии реализации двухкомпонентного стеганографического контейнера.

3) Разработка способа встраивания двухкомпонентного контейнера в покрывающий объект.

4) Разработка комплекса математических моделей подсистем встраивания сигнала сообщения в двухкомпонентный контейнер и подсистем извлечения сигнала сообщения из двухкомпонентного контейнера.

5) Разработка и обоснование способов выбора параметров двухкомпонентных стеганографических алгоритмов, обеспечивающих высокий уровень сокрытия информации и стойкости ко взлому.

6) Разработка технических решений двухкомпонентных стеганографических систем на основе результатов численного и имитационного моделирования и программного обеспечения предложенных двухкомпонентных стеганографических систем защиты информации.

При решении поставленных задач были использованы методы математического и численного моделирования, системный анализ, теория чувствительности динамических систем, метод спектрального анализа, статистические методы (в частности, корреляционный анализ), цифровая обработка сигналов (в частности, цифровая обработка звуковых сигналов и цифровая обработка растровых изображений, цифровая фильтрация), алгоритмы стеганографической защиты информации.

Анализ известных стеганографических алгоритмов

Сделан анализ существующих стеганографических алгоритмов, определены показатели устойчивости стеганографических алгоритмов, выполнена их классификация. Общая структура известных стеганографических систем приведена на рисунке 1.

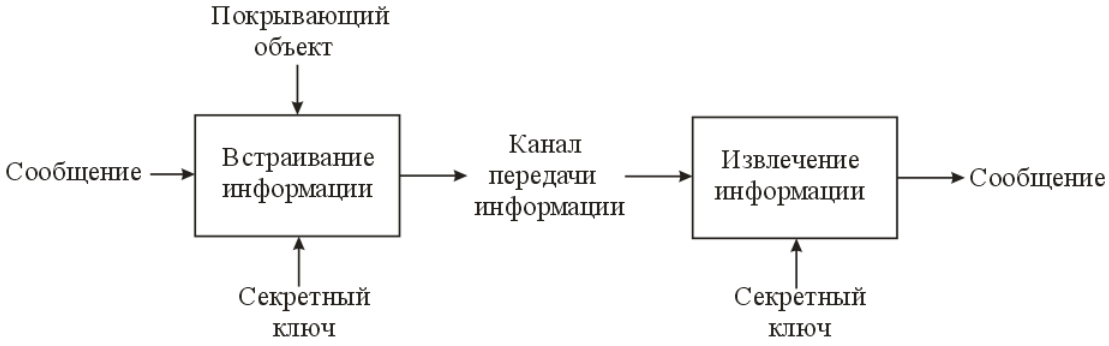


Рис. 1 Структура стеганографической системы.

Анализ стеганографических алгоритмов показал, что известные стеганографические контейнеры являются однокомпонентными и описываются выражением

$$y_i = f(u_i, \xi_i),$$

где y_i – отсчёт сигнала заполненного контейнера, u_i – скрываемое сообщение, ξ_i – отсчёт сигнала пустого контейнера. В дальнейшем индексы отсчётов i опущены.

Процесс извлечения сообщения сводится к решению уравнения с двумя неизвестными. Для решения этой задачи используют один из двух подходов встраивания сообщения.

Первый подход заключается в обнулении определённых элементов контейнера и их замещением скрываемой информацией. Например, метод наименьших значащих бит (НЗБ) и его многочисленные вариации (встраивание происходит в определённые биты контейнера), метод встраивания сообщения в фазу звукового сигнала (встраивание происходит в обнулённые отсчёты фазового спектра сегмента контейнера). Использование первого подхода позволяет точно восстановить скрытое сообщение, но обладает уязвимостью, так как области встраивания для каждого типа данных определены, и на них могут быть проведены целенаправленные атаки.

Второй подход основан на смешивании скрываемого сигнала и сигнала контейнера. Например, метод кодирования с расширением спектра для встраивания цифровых водяных знаков. Если принимающей стороне известен сигнал контейнера, то скрытый сигнал восстанавливается. В противном случае применяются статистические методы анализа, и точное восстановление сигнала не всегда возможно. Недостатком данного подхода является необходимость знания принимающей стороной сигнала контейнера.

Недостатки однокомпонентных контейнеров заключаются в том, что для обеспечения возможности восстановления сообщения накладывается значительное количество ограничений на используемый контейнер и на возможность перемешивания маскирующего сигнала и сигнала контейнера.

В работе предлагается научно-практическая концепция инвариантной стеганографической системы, отличающаяся использованием двухкомпонентного стеганографического контейнера и позволяющая реализовать абсолютную инвариантность алгоритма извлечения сообщения от сигнала контейнера, используя следующий алгоритм [10]:

$$\begin{cases} u_1(n) = f_1\big(u(n)\big), \\ u_2(n) = f_2\big(u(n)\big), \\ y_1(n) = f_3\big(u_1(n), \xi(n)\big), \\ y_2(n) = f_4\big(u_2(n), \xi(n)\big). \end{cases} \quad (1)$$

В этом случае процесс извлечения сообщения представляет собой решение двух уравнений с тремя неизвестными, две из которых являются функциями сообщения, что позволяет реализовать восстановление сообщения при произвольном сигнале контейнера и получить высокую чувствительность к вариации коэффициентов [11, 12].

Определено условие реализуемости двухкомпонентных систем, заключающееся в наличии единственного решения выражения

$$u(n) = f\big(y_1(n), y_2(n)\big) \quad (2)$$

при определённых функциях в выражении (1).

Сформулирована задача разработки методологии синтеза двухкомпонентных стеганографических систем по трём направлениям, определяемым отличиями контейнеров: когда первая компонента является сигналом пустого контейнера, а вторая компонента представляет собой функцию сигналов первой компоненты и сообщения; когда на основе покрывающего объекта

синтезируются две компоненты встраиваемой информации, и они встраиваются в покрывающий объект; когда каждая компонента представляет собой функцию двух информативных сигналов.

КОМПЛЕКС МАТЕМАТИЧЕСКИХ МОДЕЛЕЙ ДВУХКОМПОНЕНТНЫХ СТЕГАНОГРАФИЧЕСКИХ СИСТЕМ

Рассмотрены преобразования, с помощью которых формируются компоненты контейнера. Анализируются сумма [13–19], произведение [20] и отношение [21] линейных функций двух сигналов. Для каждого случая определены условия, когда выражение (2) имеет единственное решение. Далее, для сокращения записи, нумерация отсчётов *n* опущена.

Сумма линейных функций двух сигналов:

$$y = (a_1 + b_1 u_1) \pm (a_2 + b_2 u_2).$$

Раскрывая скобки и распространяя на две компоненты имеем:

$$\begin{cases} y_1 = a_1 + b_1 u_1 + c_1 \xi, \\ y_2 = a_2 + b_2 u_2 + c_2 \xi, \end{cases} \quad (3)$$

где u_1 и u_2 – встраиваемые сигналы, формируемые из сигнала сообщения определённым способом:

$$u_1 = f_1(u), \quad u_2 = f_2(u). \quad (4)$$

В работе рассматриваются два вида связи встраиваемых сигналов и сигнала сообщения – аддитивный и мультипликативный. Аддитивный вид связи:

$$u_1 = u, \quad u_2 = K - u. \quad (5)$$

Мультипликативный вид связи:

$$u_1 = u, \quad u_2 = u_1/K. \quad (6)$$

Встраиваемый сигнал u_1 эквивалентен сигналу сообщения, и в дальнейшем будем называть его сообщением.

При использовании алгоритма встраивания (3) и вида связи (5) выражение для извлечения сообщения имеет вид:

$$u_1 = \frac{Kb_2c_1 - a_1c_2 + a_2c_1 - c_1y_2 + c_2y_1}{b_1c_2 + b_2c_1}. \quad (7)$$

При использовании алгоритма встраивания (3) и вида связи (6) выражение для извлечения сообщения имеет вид

$$u_1 = \frac{K(a_2c_1 - a_1c_2 + c_2y_1 - c_1y_2)}{Kb_1c_2 - b_2c_1}.$$

Произведение линейных функций двух сигналов:

$$y = (a_1 + b_1 u_1)(a_2 + b_2 u_2).$$

Раскрывая скобки и распространяя на две компоненты имеем:

$$\begin{cases} y_1 = a_1 + b_1 u_1 + c_1 \xi + g_1 u_1 \xi, \\ y_2 = a_2 + b_2 u_2 + c_2 \xi + g_2 u_2 \xi. \end{cases} \quad (8)$$

При использовании алгоритма встраивания (8) и вида связи (5) при извлечении сообщения возникает неопределённость, которая исключается, если ввести условие:

$$b_1 g_2 = b_2 g_1. \quad (9)$$

Выражение для извлечения сообщения примет вид

$$u_1 = -\frac{K(-b_2c_1-g_2y_1+g_2a_1)+a_1c_2-a_2c_1+c_1y_2-c_2y_1}{b_1c_2+b_2c_1-a_1g_2-a_2g_1+g_1y_2+g_2y_1}.$$

При использовании алгоритма встраивания (8) и вида связи (6) также возникает неопределённость, которая исключается условием (9). Выражение для извлечения сообщения принимает вид

$$u_1 = \frac{K(-a_1c_2+a_2c_1-c_1y_2+c_2y_1)}{K(b_1c_2+g_1y_2-g_1a_2)-b_2c_1-g_2y_1+g_2a_1}.$$

Отношение линейных функций двух сигналов:

$$y = \frac{a_1+b_1u_1}{a_2+b_2u_2}.$$

В зависимости от того, какой сигнал является встраиваемым, принимает один из двух видов. Первая модель:

$$\begin{cases} y_1 = \frac{1+a_1u_1}{b_1+c_1\xi}, \\ y_2 = \frac{1+a_2u_2}{b_2+c_2\xi}. \end{cases} \quad (10)$$

Вторая модель:

$$\begin{cases} y_1 = \frac{1+a_1\xi}{b_1+c_1u_1}, \\ y_2 = \frac{1+a_2\xi}{b_2+c_2u_2}. \end{cases} \quad (11)$$

При использовании алгоритма встраивания (10) и вида связи (5) выражение для извлечения сообщения имеет вид

$$u_1 = \frac{a_2c_1y_1K+c_1y_1-c_2y_2-y_1y_2(b_2c_1-b_1c_2)}{a_1c_2y_2+a_2c_1y_1}.$$

При использовании алгоритма встраивания (10) и вида связи (6) выражение для извлечения сообщения имеет вид

$$u_1 = K\frac{c_1y_1-c_2y_2-y_1y_2(b_2c_1-b_1c_2)}{a_1c_2y_2K-a_2c_1y_1}.$$

При использовании алгоритма встраивания (11) и вида связи (5) выражение для извлечения сообщения имеет вид:

$$u_1 = -\frac{a_1-a_2-a_1b_2y_2+a_2b_1y_1-a_1c_2y_2K}{a_1c_2y_2+a_2c_1y_1}.$$

При использовании функции (11) и вида связи (6) выражение для извлечения сообщения имеет вид:

$$u_1 = K\frac{-a_1+a_2+a_1b_2y_2-a_2b_1y_1}{a_2c_1y_1K-a_1c_2y_2}.$$

Также рассматривается вариант формирования компонент путём **взаимного смешивания независимых сигналов**.

В этом случае выражение (3) преобразуется к виду

$$\begin{cases} y_1 = a_1 + b_1u_1 + c_1u_2, \\ y_2 = a_2 + b_2u_2 + c_2u_1. \end{cases}$$

Выражения для извлечения встраиваемых сигналов имеют вид

$$u_1 = \frac{a_2c_1-a_1b_2-c_1y_2+b_2y_1}{b_1b_2-c_1c_2}; \qquad u_2 = \frac{a_1c_2-a_2b_1-c_2y_1+b_1y_2}{b_1b_2-c_1c_2}.$$

Выражение (8) преобразуется к виду

$$\begin{cases} y_1 = a_1 + b_1u_1 + c_1u_2 + g_1u_1u_2, \\ y_2 = a_2 + b_2u_2 + c_2u_1 + g_2u_1u_2. \end{cases} \quad (12)$$

Неопределённость решения устраняется условием

$$b_1g_2 - c_2g_1 = 0,$$

при выполнении условия получим:

$$u_1 = \frac{-a_1b_2+a_2c_1+b_2y_1-c_1y_2}{a_1g_2-a_2g_1+b_1b_2-c_1c_2+g_1y_2-g_2y_1}. \quad (13)$$

Для извлечения сигнала u_2 используется (12) и результат (13):

$$u_2 = \frac{y_1-a_1-b_1u_1}{c_1+g_1u_1}.$$

На основе отношения линейных функций двух сигналов алгоритм встраивания имеет вид

$$\begin{cases} y_1 = \dfrac{1 + a_1u_1}{b_1 + c_1u_2}, \\ y_2 = \dfrac{1 + a_2u_2}{b_2 + c_2u_1}. \end{cases}$$

Выражения для извлечения сигналов имеют вид

$$u_1 = \frac{a_2-a_2b_1y_1+c_1y_1-b_2c_1y_1y_2}{c_2y_1y_2-a_1a_2}; \quad u_2 = \frac{a_1-a_1b_2y_2+c_2y_2-b_1c_2y_1y_2}{c_1y_1y_2-a_1a_2}.$$

Полученные математические модели полностью описывают подсистемы встраивания и извлечения сообщений в общем виде, а также определяют условия, при которых происходит однозначное извлечение сообщений.

Исследование разработанных математических моделей

Так как сигнал сообщения может быть легко обнаружен злоумышленником, знающим используемый алгоритм сокрытия (из-за свойства инвариантности), то обеспечить дополнительную защиту позволяют ключевые коэффициенты. Это коэффициенты, минимальная ошибка в значении которых приводит к максимальному подавлению скрытого сообщения.

С этой целью для каждой из полученных математических моделей определяется условие максимальной чувствительности к вариации коэффициентов [22–24]. Функции извлечения сигнала представляют собой дроби, поэтому максимальная чувствительность к вариации коэффициентов наблюдается вблизи точки разрыва функции. Принимая отклонение знаменателя от нуля за σ, получены условия максимальной чувствительности для каждой модели с учётом условий реализуемости этих моделей.

Для моделей, основанных на сумме линейных функций двух сигналов при использовании аддитивного вида связи (4), условие максимальной чувствительности определяется выражением:

$$\begin{cases} b_1c_2 + b_2c_1 = \sigma \\ \text{при} \quad \sigma \to 0. \end{cases} \quad (14)$$

Количество коэффициентов функции извлечения равно шести. Помимо этого, используется значение K. Выражение для абсолютной чувствительности функции извлечения сообщения стеганографической системы на основе суммы линейных функций двух сигналов имеет следующий вид:

$$\Delta_{u_1} = S_{a_1}\Delta_{a_1} + S_{a_2}\Delta_{a_2} + S_{b_1}\Delta_{b_1} + S_{b_2}\Delta_{b_2} + S_{c_1}\Delta_{c_1} + S_{c_2}\Delta_{c_2} + S_K\Delta_K, \quad (15)$$

где Δ – приращения соответствующей величины, S – чувствительность системы к вариации соответствующей величины.

Знаменатель выражения (7) не содержит принимаемые сигналы y_1 и y_2, поэтому рабочая точка алгоритма восстановления фиксирована. Очевидно, что чем меньше значение σ, тем ближе рабочая точка системы к точке разрыва и тем выше чувствительность системы к вариации коэффициентов.

В качестве примера покажем выражения коэффициентов чувствительности S для (14). Используем производные по всем коэффициентам:

$$S_{a_1} = \frac{du_1}{da_1} = -\frac{c_2}{b_1c_2+b_2c_1}; \tag{16}$$

$$S_{a_2} = \frac{du_1}{da_2} = \frac{c_1}{b_1c_2+b_2c_1}; \tag{17}$$

$$S_{b_1} = \frac{du_1}{db_1} = \frac{c_2(-a_1c_2+a_2c_1-c_1y_2+c_2y_1+Kb_2c_1)}{(b_1c_2+b_2c_1)^2}; \tag{19}$$

$$S_{b_2} = \frac{du_1}{db_2} = \frac{c_1(a_1c_2-a_2c_1+c_1y_2-c_2y_1+Kb_1c_2)}{(b_1c_2+b_2c_1)^2}; \tag{19}$$

$$S_{c_1} = \frac{du_1}{dc_1} = \frac{c_2(a_1b_2+a_2b_1-b_1y_2-b_2y_1+Kb_1b_2)}{(b_1c_2+b_2c_1)^2}; \tag{20}$$

$$S_{c_2} = \frac{du_1}{dc_2} = -\frac{c_1(a_1b_2+a_2b_1-b_1y_2-b_2y_1+Kb_1b_2)}{(b_1c_2+b_2c_1)^2}; \tag{21}$$

$$S_K = \frac{du_1}{dK} = \frac{b_2c_1}{b_1c_2+b_2c_1}. \tag{22}$$

Значения y_1 и y_2 хоть и содержат в себе значения всех коэффициентов, однако принимающая сторона получает их в виде текущих отсчётов. При дифференцировании y_1 и y_2 не раскрываются.

Выражения (16), (17) и (22) не зависят от соответствующих варьируемых коэффициентов, поэтому погрешность извлечения будет линейной функцией варьируемого коэффициента.

Выражения (18)–(21) представляют собой гиперболические зависимости.

Зная коэффициенты преобразования (3) с помощью выражений (16)–(22) оценивается чувствительность системы к вариации того или иного коэффициента, и выбирается коэффициент наиболее подходящий на роль ключевого коэффициента, который является секретным.

На рисунке 2 приведена зависимость ошибки извлечения сигнала от вариации коэффициентов *a, b, c* и *K*.

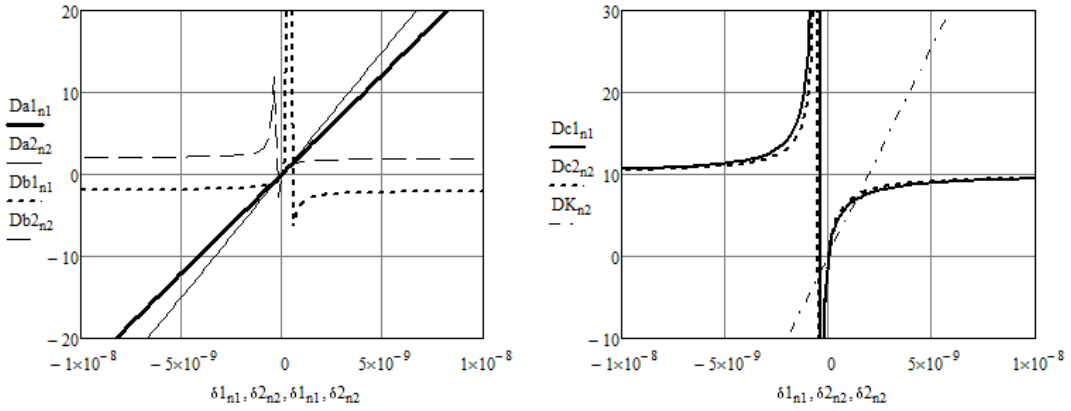


Рис. 2 Зависимость ошибки извлечения сигнала сообщения от вариации коэффициентов.

По оси абсцисс откладывается вносимая в значение соответствующего коэффициента погрешность, по оси ординат откладывается абсолютная ошибка извлечения сообщения. Так как значение сообщения $u_1 = 2$, ошибка извлечения как при использовании коэффициентов *a,*

так и при использовании коэффициентов b может считаться достаточной. Однако ошибка извлечения сигнала при использовании коэффициентов a в качестве ключа сравнительно больше и не приводит к формированию разрыва функции (7). Погрешность извлечения сообщения при использовании в качестве ключа коэффициента K больше, чем при использовании коэффициентов a, и также имеет линейный характер. Погрешность извлечения сообщения при использовании в качестве ключа коэффициентов c имеет такой же характер, как и при использовании коэффициентов b, однако она значительно больше.

Проведён анализ всех алгоритмов, и получены выражения, позволяющие оценить чувствительность стеганографической системы к вариации тех или иных ключевых коэффициентов. Важно отметить, что условия максимальной чувствительности в ряде алгоритмов зависят от величин принимаемых сигналов.

Получены результаты численных исследований разработанных моделей с целью определения эффективности сокрытия сигнала и влияния ошибки, вносимой в коэффициенты, на точность извлечения сигнала.

Так как основная задача ключевого коэффициента – это обеспечение скрытности встроенного сигнала при наличии ошибки в значении коэффициента, то важны не только абсолютная ошибка в значении сигнала, но и характер вносимого искажения. Исследования показали, что разные коэффициенты вносят различные искажения в извлечённый сигнал.

Для наглядности определения, какой из коэффициентов наиболее эффективно использовать в качестве ключевого, определён характер искажения извлечённого полезного сигнала при внесении ошибки в тот или иной коэффициент. Для этого использовано численное моделирование.

Например, зададимся исходными значениями:

$$a_1 = 0{,}1;\ a_2 = 0{,}3;\ b_1 = -2{,}1;\ b_2 = 1{,}7;\ c_1 = 3;\ K = 0{,}2;\ \sigma = 1 \times 10^{-9}.$$

С помощью (39) найдём c_2:

$$c_2 = \frac{\sigma - b_2 c_1}{b_1} = 2{,}429.$$

Формируя случайный сигнал сообщения и маскирующий сигнал, реализуем стеганографическую систему в соответствии с (3) и при восстановлении полезного сигнала с помощью (7) внесём ошибку в соответствующие коэффициенты.

На рисунке 3, *а* приведены зависимости маскирующего сигнала ξ и сигналов передаваемых компонент y_1 и y_2. Видно, что форма сигналов компонент сходна с формой маскирующего сигнала. При заданных параметрах системы коэффициенты корреляции компонент и полезного сигнала равны 0,22, что говорит о достаточно эффективной маскировке сигнала. При внесении в значения коэффициентов ошибки равной $\delta = 1 \times 10^{-10}$ получены зависимости, приведённые далее. Заметим, что характер зависимостей при внесении ошибки в коэффициенты первой и второй компонент сходны. Поэтому на рисунках представлены только зависимости, полученные при внесении ошибки в коэффициенты первой компоненты.

На рисунке 3, *б* приведены графики встроенного и извлечённого сигналов при внесении ошибки в коэффициент a_1. Видно, что в этом случае появляется постоянная составляющая, которая легко исключается из сигнала. Следовательно, использование в качестве ключевых коэффициентов a в данном алгоритме восстановления исключается. Аналогичный результат получен и при внесении ошибки в коэффициент K.

На рисунке 3, *в* приведены графики встроенного и извлечённого сигналов при внесении ошибки в коэффициент b_1. Видно, что в этом случае изменяется амплитуда восстановленного сигнала, что легко корректируется. Следовательно, использование в качестве ключевых коэффициентов b в данном алгоритме восстановления также исключается.

На рисунке 3, *г* приведены графики встроенного и извлечённого сигналов при внесении погрешности в коэффициент c_1. Видно, что в этом случае информативный сигнал маскируется

случайным сигналом, что говорит об эффективности использования в качестве ключевых коэффициентов *c*.

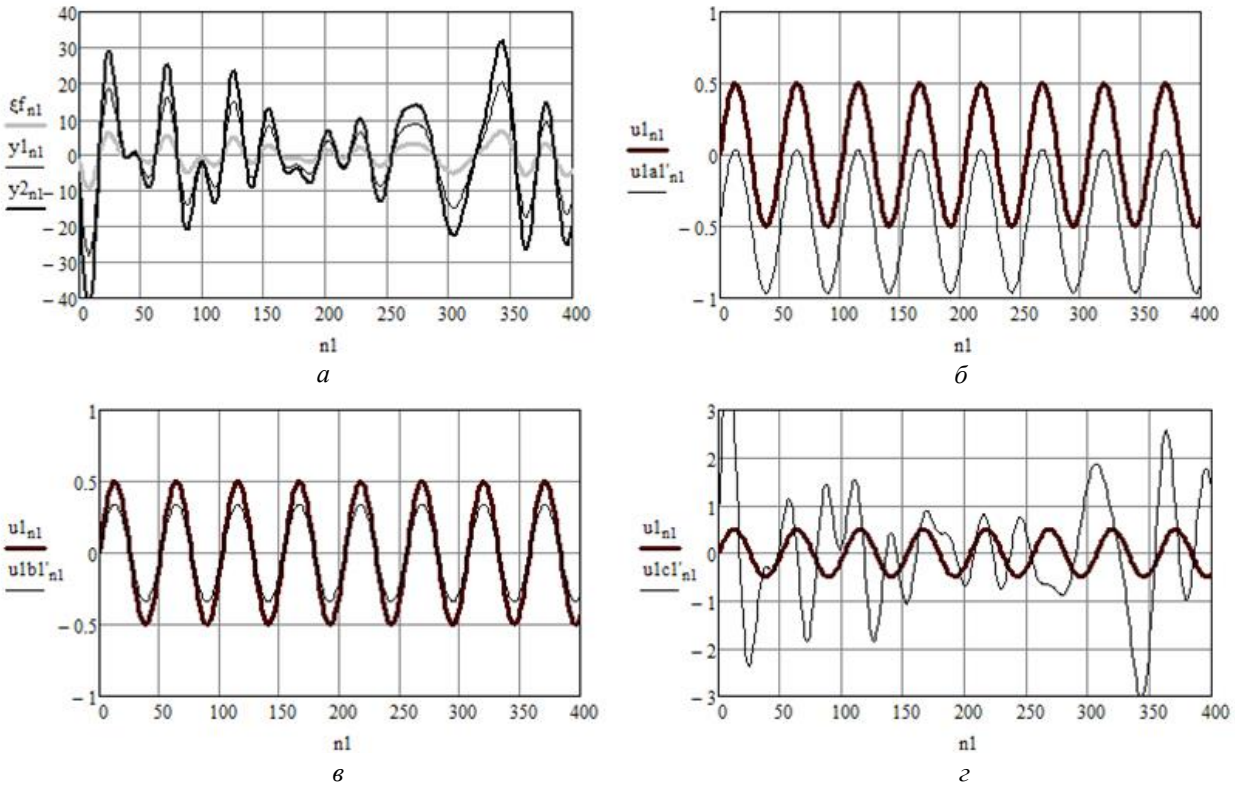


Рис. 3 Зависимости:
а – маскирующего сигнала ξ и сигналов передаваемых компонент y_1 и y_2;
б – встроенного и извлечённого сигналов при внесении ошибки в коэффициент a_1;
в – встроенного и извлечённого сигналов при внесении ошибки в коэффициент b_1;
г – встроенного и извлечённого сигналов при внесении погрешности в коэффициент c_1.

Рассмотрим влияние изменения ошибки значения коэффициента *c* на спектр извлечённого сигнала. На рисунке 4 приведена поверхность, показывающая изменение спектра извлечённого сигнала от ошибки $\delta\times10^{-11}$ в значении коэффициента c_1. Видно, что при нулевой ошибке спектр состоит из одной гармоники. При увеличении ошибки гармоника извлечённого сигнала скрывается в спектре маскирующего сигнала.

Отметим, что при значении $\sigma = 1\times10^{-9}$ и при ошибке значения $c_1 = 20\times10^{-11}$ гармоника извлечённого сигнала полностью скрывается в спектре маскирующего сигнала.

Аналогичным образом проведено моделирование всех разработанных алгоритмов. Проведённый анализ показал, что в каждом из алгоритмов существует коэффициент, обеспечивающий достаточный уровень устойчивости стеганографической системы. Важно заметить, что при ограничении разрядности представления данных вариабельность коэффициентов ограничивается. Использование условий реализуемости системы, например, условие (9) вкупе с условием максимальной чувствительности системы, например, условие (14), могут сильно ограничить поиск значения одного коэффициента, и сделать систему уязвимой. Поэтому для каждого из алгоритмов определены группы ключевых коэффициентов, рекомендуемые для хранения в тайне. Дополнительно указаны коэффициенты, ошибка в которых вызывает наибольшее искажение восстановленного сообщения. Результаты сведены в таблицу 1.

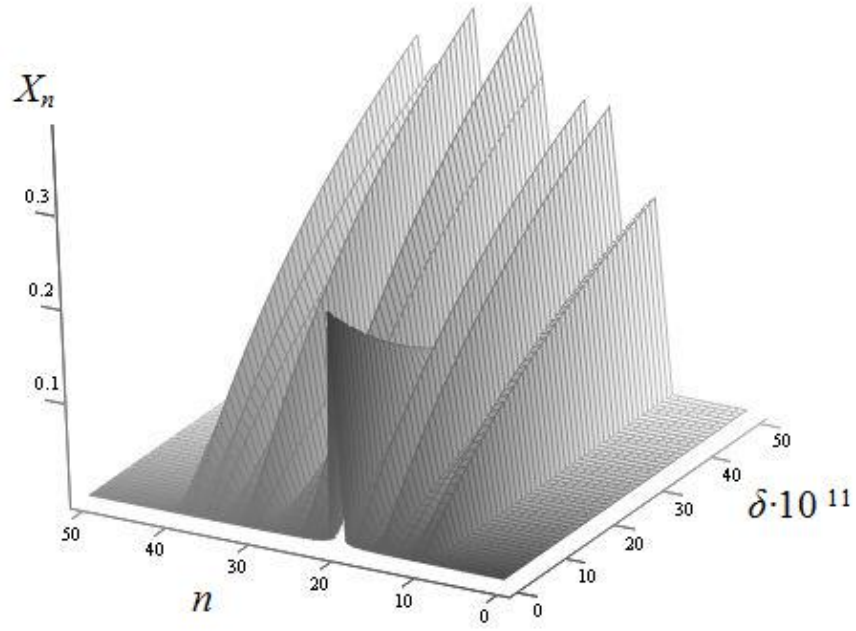


Рис. 4 Изменение спектра извлечённого сигнала от ошибки δ в значении коэффициента c_1.

Таблица 1

Ключевые коэффициенты стегосистем

№ п/п	Алгоритм	Группа ключевых коэффициентов	Рекомендуемые ключевые коэффициенты
1	На основе суммы линейных функций двух сигналов с аддитивной связью встраиваемых сигналов	b_1, b_2, c_1, c_2	c_1 и c_2
2	На основе суммы линейных функций двух сигналов с мультипликативной связью встраиваемых сигналов	b_1, b_2, c_1, c_2, K	c_1 и c_2
3	На основе произведения линейных функций двух сигналов с аддитивной связью встраиваемых сигналов	c_1, c_2, g_1, g_2, K	c_1, c_2, g_1 и g_2
4	На основе произведения линейных функций двух сигналов с мультипликативной связью встраиваемых сигналов	c_1, c_2, g_1, g_2, K	g_1 и g_2
5	На основе отношения линейных функций двух сигналов с аддитивной связью встраиваемых сигналов (модель 1)	a_1, a_2, c_1, c_2, K	c_1 и c_2
6	На основе отношения линейных функций двух сигналов с аддитивной связью встраиваемых сигналов (модель 2)	a_1 и a_2	a_1 и a_2
8	На основе отношения линейных функций двух сигналов с мультипликативной связью встраиваемых сигналов (модель 1)	a_1, a_2, c_1, c_2, K	c_1 и c_2
9	На основе отношения линейных функций двух сигналов с мультипликативной связью встраиваемых сигналов (модель 2)	a_1 и a_2	a_1 и a_2

Для алгоритмов, использующих взаимную маскировку сигналов, ключевые коэффициенты сведены в таблицу 2.

Таблица 2

Ключевые коэффициенты стегосистем со взаимной маскировкой

№ п/п	Алгоритм	Группа ключевых коэффициентов	Рекомендуемые ключевые коэффициенты
1	На основе суммы линейных функций двух сигналов	b_1, b_2, c_1, c_2	b_2 или c_1 b_1 или c_2
2	На основе произведения линейных функций двух сигналов	b_2, c_1, g_1, g_2	c_2, и g_1
3	На основе отношения линейных функций двух сигналов	a_1, b_2, c_1, c_2	a_2 и c_1

Структурные схемы стеганографических систем

Рассмотрим разработанные на основе математических моделей структурные схемы стеганографических систем и проведем их имитационное моделирование. Рассмотрены два подхода к построению стеганографического кодера.

Первый подход основан на непосредственном встраивании сигнала сообщения в сигнал контейнера. Укрупнённая структурная схема такой стеганографической системы приведена на рисунке 5.

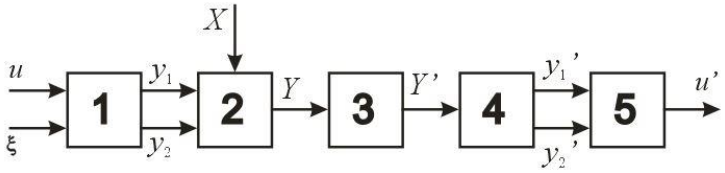


Рис. 5 Стеганографическая система
с непосредственным встраиванием сообщения в контейнер.

На вход блока стеганографического кодера *1* поступает сигнал сообщения *u* и маскирующий сигнал ξ. Заметим, что маскирующий сигнал ξ может быть как сигналом маскировки, так и сигналом пустого контейнера. На выходе первого блока формируются две компоненты y_1 и y_2, которые передаются на блок *2*, осуществляющий формирование передаваемого сигнала заполненного контейнера. Данный блок может отсутствовать в системе, если y_1 и y_2 передаются по каналу связи непосредственно. Также, если сигнал ξ является маскирующим, и подразумевается последующее встраивание компонент в сигнал пустого контейнера, на вход блока встраивания *2* подаётся сигнал пустого контейнера *X*. На выходе блока *2* формируется сигнал заполненного контейнера *Y*, который передаётся на линию связи *3*. Принимающая сторона получает сигнал *Y'*, поступающий на блок извлечения компонент *4*, который также может отсутствовать, если y_1 и y_2 передаются по каналу связи непосредственно. На выходе блока извлечения компонент *4* формируются сигналы компонент y_1' и y_2', поступающие на блок стеганографического декодера *5*, на выходе которого формируется сигнал сообщения *u*'. В рамках данной статьи рассматривается формирование блока *1*, стеганографического кодера и блока *5*, стеганографического декодера.

Аналогичным образом работает стеганографическая система при взаимной маскировке компонент (рисунок 6), с той лишь разницей, что на вход стеганографического кодера подаются два встраиваемых сигнала u_1 и u_2. В блоке декодера извлекаются оба замаскированных сигнала.

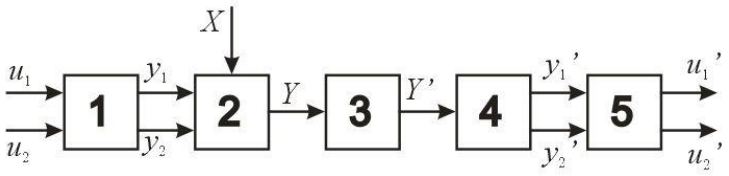


Рис. 6 Стеганографическая система со взаимной маскировкой сигналов.

Второй подход основан на синтезе маскирующего сигнала из сигнала контейнера. Структурная схема стеганографической системы с синтезируемым маскирующим сигналом приведена на рисунке 7.

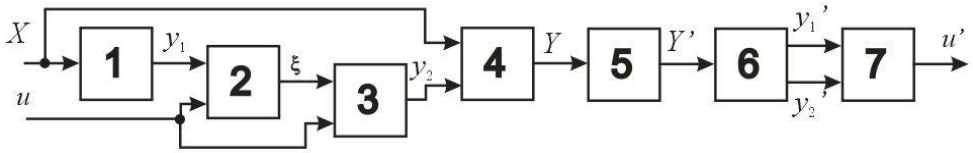


Рис. 7 Стеганографическая система с синтезом маскирующего сигнала из сигнала контейнера.

На вход системы подаются сигнал пустого контейнера и сигнал сообщения. Подразумевается, что первая компонента y_1 имеет значение области встраивания контейнера. Таким образом, в блоке *1* определяется значение компоненты y_1 как значение соответствующей области сигнала *X*. Блок *2* определяет значение маскирующего сигнала ξ с помощью выражения для формирования компоненты y_1, значения y_1 и значения сообщения *u*. Блок *3* формирует значение компоненты y_2 с помощью полученного значения ξ и значения сообщения *u* в соответствии с алгоритмом формирования y_2. В блоке *4* происходит встраивание второй компоненты y_2 в контейнер *X*. Сигнал заполненного контейнера *Y*, получаемый на выходе блока *4*, передаётся на линию связи *5*. С линии связи сигнал стеганографического контейнера передаётся на вход блока выделения компонент *6*, откуда поступает на блок стеганографического декодера *7*. На выходе декодера *7* формируется извлечённый сигнал сообщения *u*'.

Подсистема встраивания информации для первого подхода содержит блок *1* (см. рисунки 5 и 6). Подсистема извлечения информации содержит блок *5*. Подсистема встраивания информации для второго подхода содержит блоки *2* и *3* (см. рисунок 7). Подсистема извлечения информации содержит блок *7*.

Каждой математической модели соответствуют две структурных схемы – структурная схема кодера, обеспечивающего формирование двух компонент передаваемого сигнала, и структурная схема декодера, обеспечивающего извлечение полезного сигнала из контейнера. Структурные схемы построены на основе блоков простых математических операций – сложения, вычитания, умножения и деления [18, 19, 26, 27].

На рисунке 8 приведена структурная схема стеганографического кодера для стеганографической системы, изображенной на рисунке 5, и построенной на основе суммы линейных функций двух сигналов, использующей аддитивный вид связи встраиваемых сигналов. Структурная схема состоит из блока памяти *1* коэффициентов, блоков суммирования *2, 7* и *8*, блоков умножения *3–6*. На вход кодера поступают сигналы u_1 и ξ, на выход передаются компоненты заполненного контейнера y_1 и y_2.

Рассмотрим кодер, построенный в соответствии со структурной схемой, представленной на рисунке 7. Процесс кодирования проходит в два этапа. На первом этапе, в блоке 2, из выделенного сигнала y_1 происходит формирование сигнала ξ. На втором этапе, в блоке 3, формируется сигнал второй компоненты y_2. Выделение сигнала ξ из сигнала y_1 происходит в соответствии с первым выражением (5) следующим образом: $\xi = \frac{y_1 - a_1 - b_1 u_1}{c_1}$.

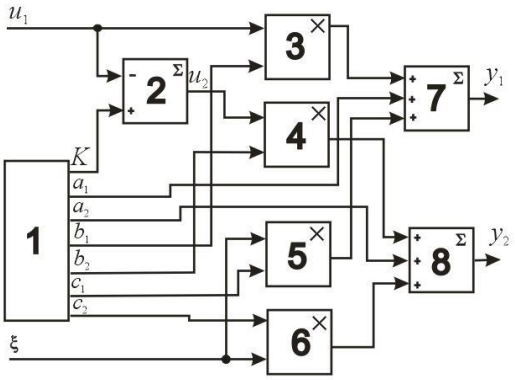
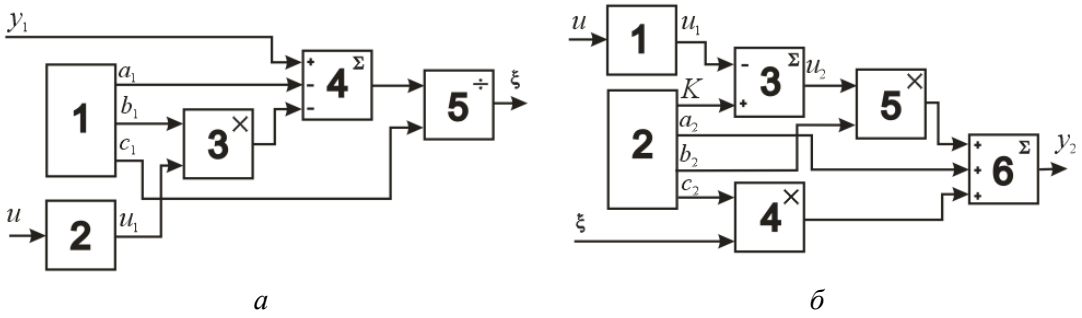


Рис. 8 Стеганографический кодер.

Структурная схема блока выделения сигнала ξ представлена на рисунке 9, *а*. Структурная схема содержит блок *1* памяти коэффициентов; блок *2*, формирующий сигнал u_1 из сигнала сообщения u; блок умножения *3*; блок суммирования *4*; блок деления *5*. На выходе структурной схемы формируется маскирующий сигнал ξ.

Структурная схема блока, формирующего сигнал второй компоненты y_2 (блока *3*, структурной схемы, представленной на рисунке 7), представлена на рисунке 9, *б*. На вход структурной схемы подаются сигнал сообщения u и маскирующий сигнал ξ. Структурная схема содержит блок *1*, формирующий встраиваемый сигнал u_1 из сигнала сообщения u; блок *2* памяти коэффициентов; блоки сложения *3* и *6*; блоки умножения *4* и *5*. На выходе структурной схемы формируется сигнал второй компоненты y_2.

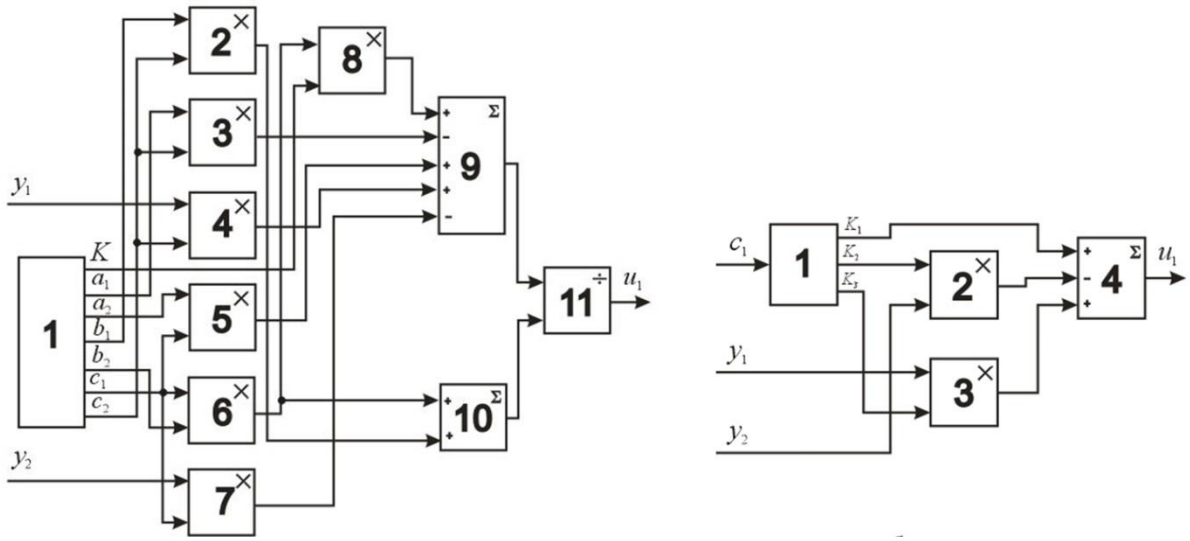


а *б*

Рис. 9 Структурные схемы блоков:
а – синтеза маскирующего сигнала; *б* – формирования второй компоненты.

На рисунке 10, *а* приведена структурная схема декодера стеганографической системы. На вход декодера поступают сигналы двух компонент заполненного контейнера y_1 и y_2. На выходе формируется сигнал u_1. Декодер состоит из блока памяти коэффициентов *1*, блоков умножения *2 – 8*, блоков суммирования *9* и *10*, блока деления *10*.

Данные структурные схемы построены на основе математических моделей без оптимизации вычислений. Однако при неизменности коэффициентов преобразования большая часть вычислений в декодере может быть выполнена однократно. На рисунке 10, *б* приведена структурная схема декодера, построенная с учётом сокращения математических операций. Блок *1* является блоком предварительного расчёта коэффициентов, блоки *2* и *3* – умножители, блок *4* – блок суммирования.



а *б*

Рис. 10 Стеганографический декодер:
а – общая структурная схема; *б* – схема декодера
с предварительно рассчитанными коэффициентами.

Блок предварительного расчёта коэффициентов передаёт на выход следующие коэффициенты, которые описываются выражениями

$$K_1 = \frac{Kb_2c_1 - a_1c_2 + a_2c_1}{b_1c_2 + b_2c_1}; \quad K_2 = \frac{c_1}{b_1c_2 + b_2c_1}; \quad K_3 = \frac{c_2}{b_1c_2 + b_2c_1}.$$

Для стеганографических систем на основе взаимной маскировки компонент для моделей, основанных на произведении и отношении линейных функций двух сигналов, дополнительно разработаны структурные схемы декодера второго скрытого сигнала, что обусловливается его получением с использованием восстановленного сигнала u_1.

Все разработанные структурные схемы исследованы с помощью моделей в среде MATLAB–Simulink [28, 29]. На основные структурные схемы получены патенты. На рисунке 11 приведена компьютерная модель стеганографической системы.

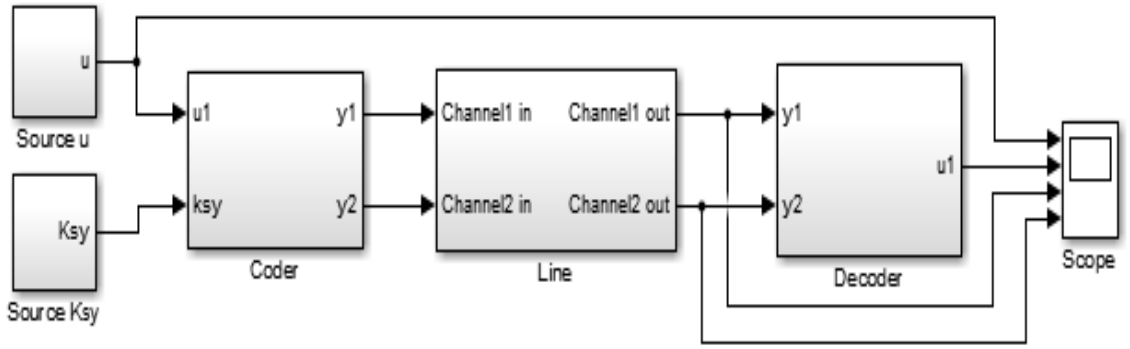


Рис. 11 Модель стеганографической системы в среде MATLAB.

Модель состоит из источников полезного сигнала, сигнала контейнера и ключевого коэффициента, передающихся в блок стеганографического кодера, раскрытого на рисунке 12, *а*. На выходе кодера формируются две компоненты стеганографического контейнера, передаваемые по линии

связи и поступающие в блок декодера, раскрытый на рисунке 12, *б*. На выходе декодера формируется восстановленный сигнал u_1.

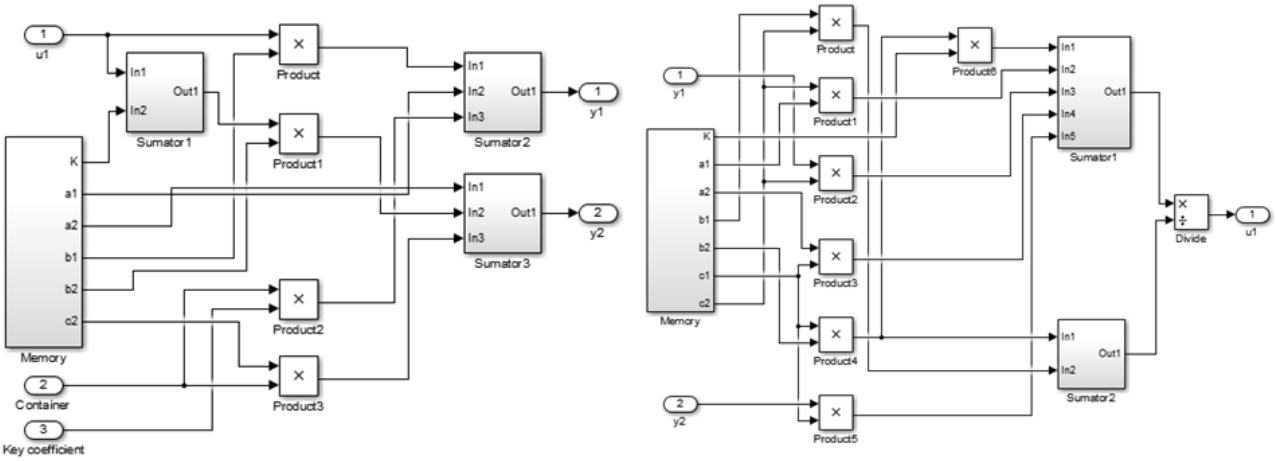


Рис. 12 Модели:
а – стеганографического кодера; *б* – стеганографического декодера.

Проведённое имитационное моделирование позволило сделать важные выводы об особенностях работы каждой из разработанных стеганографических систем в условиях ограничения разрядности представления данных.

Практическая реализация и внедрение разработанных стеганографических систем

На основе полученных математических моделей разработаны методы встраивания информации в контейнеры с большой разрядностью представления данных и в контейнеры с ограниченной разрядностью представления данных.

Использование контейнеров с большой разрядностью представления данных (числа с плавающей запятой) эффективным методом является непосредственное встраивание на основе полученных математических моделей. Так, для ООО НПФ «Автоматические системы контроля» для передачи скрытой информации использован канал передачи результатов измерений с последующим восстановлением измеренных и встроенных данных.

Использование чисел с плавающей запятой позволяет получить большую вариабельность ключевых коэффициентов и обеспечить достаточно эффективную маскировку скрытой информации и сложность её извлечения.

Для защищённой передачи информации в центр обработки данных, распознавания и оперативного анализа для организации ООО «Открытый код» разработан алгоритм встраивания служебной информации в передаваемые изображения на основе метода наименьших значащих бит (НЗБ). Использование полученных математических моделей для непосредственного встраивания сообщений в растровые изображения оказалось малоэффективным по ряду причин:

- необходимость снижения амплитуды отсчётов изображения, что приводит к искажению плотности распределения вероятности заполненного контейнера и высокой заметности встраивания;
- ограничение значений ключевых коэффициентов, не позволяющее обеспечить дополнительную защиту от извлечения.

Экспериментальные исследования показали [30], что использование структуры, изображенной на рисунке 7, позволяет осуществить эффективное встраивание двухкомпонентного контейнера в покрывающее изображение. Предложен способ формирования двухкомпонентного контейнера,

первая компонента которого полностью скрывается в покрывающем изображении, а вторая встраивается с использованием метода НЗБ или его модификаций. Рассмотрены три варианта реализации. Первый вариант использует контейнеры с амплитудой три бита, второй и третий варианты используют контейнер с амплитудой 1 бит. Результаты численного анализа сокрытия сообщений с помощью дивергенции Кульбака–Лейблера по отношению к методу НЗБ сведены в таблицу 3.

Таблица 3

Дивергенция Кульбака–Лейблера между исходным покрывающим изображением и стеганографическим контейнером

Слой компоненты y_1 (наименьший)	Встраивание с использованием трёх бит	Встраивание с использованием одного бита:		Встраивание с использованием метода НЗБ
		соседний пиксель	тот же пиксель	
1	2	3	4	5
1	—	290	297 / 111*	298
2	5203	232	255 / 107*	
3	4408	215	298 / 90*	
4	3102	134	269 / 97*	
5	1495	103	302 / 97*	
6	2369	94	307 / 74*	
7	870	94	267 / 90*	
8	899	77	— / —	

Первый рассмотренный вариант встраивания показал достаточно слабое сокрытие (см. таблицу 3, столбец 2). Второй вариант встраивания однобитного контейнера (см. таблицу 3, столбец 3) подразумевал использование в качестве источника первой компоненты одних пикселей, а встраивание второй компоненты происходило в другие пиксели. Дивергенция Кульбака–Лейблера при использовании такого подхода достаточно низкая, однако использование такого подхода несколько ограничивает потенциальную пропускную способность и приводит к лучшим результатам при использовании младших бит в качестве источника сигнала первой компоненты. Третий вариант встраивания сходен со вторым, но использует в качестве источника сигнала первой компоненты пиксели, в которые производится встраивание второй компоненты (см. таблицу 3, столбец 4 без звёзд). Видно, что такой подход менее эффективен, поэтому предложена его модификация, когда формируется массив значений старших бит тех же пикселей, куда производится встраивание второй компоненты, и выполняется его перемешивание (см. таблицу 3, столбец 4 со звездой). Данный вариант встраивания менее зависим от слоя, в котором располагается первая компонента контейнера, а процесс извлечения требует выполнения перемешивания, что представляет сложную задачу для злоумышленника.

Для визуальной оценки незаметности встраивания на рисунке 13 представлены сообщение и младшие битные слои, содержащие сообщение, встроенное методом НЗБ и согласно рассмотренным однобитным алгоритмам без перемешивания и с перемешиванием.

В рамках исследования проведены эксперименты по извлечению сигнала сообщения в случае ошибки в алгоритме (координата первой компоненты или ошибка перемешивания). В результате выявлено, что скрытое расположение первой компоненты обеспечивает высокую устойчивость системы к извлечению сообщения. Так, при ошибке в координатах или при ошибке в формировании ряда случайных чисел, на котором основано перемешивание, извлекаемый сигнал значительно отличается от встроенного сообщения.

Таким образом, совместное использование двухкомпонентного контейнера с известными стеганографическими методами позволяет значительно повысить уровень защиты информации.

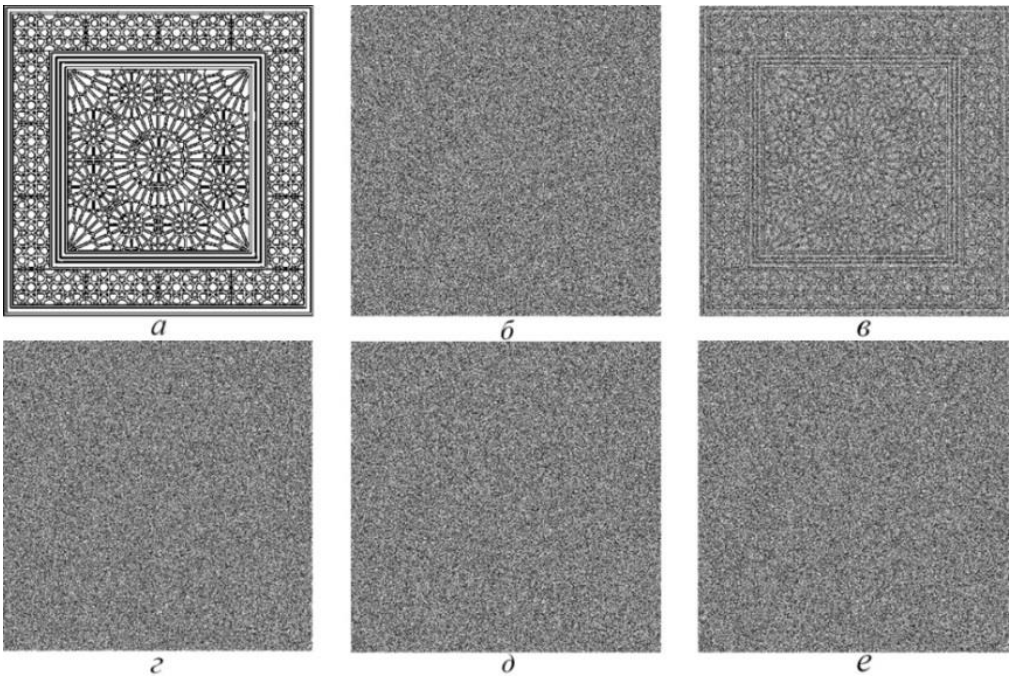


Рис. 13 Младшие битные слои:
а – сообщения; *б* – покрывающего изображения; *в* – стегоконтейнера НЗБ; *г* – двухкомпонентного стегоконтейнера (вариант 2); *д* – двухкомпонентного стегоконтейнера (вариант 3) без перемешивания; *е* – двухкомпонентного стегоконтейнера (вариант 2) с перемешиванием.

Заключение

Таким образом, решена важная научно-техническая задача, заключающаяся в повышении эффективности защиты информации посредством цифровой стеганографии через разработку и реализацию концепции абсолютно инвариантной стеганографической системы на основе синтеза двухкомпонентного контейнера.

1. Разработана научно-практическая концепция абсолютно инвариантной стеганографической системы. К основным свойствам разработанной стеганографической системы относятся: независимость алгоритма извлечения сообщения от сигнала пустого контейнера; использование как линейных, так и нелинейных алгоритмов встраивания сигнала сообщения в сигнал пустого контейнера; работа системы в реальном времени. Абсолютная инвариантность стеганографической системы достигается за счёт использования двухкомпонентного стеганографического контейнера. Сформулированы требования к абсолютно инвариантной стеганографической системе, заключающиеся в том, что алгоритм извлечения сигнала должен давать однозначный результат (единственность решения); при произвольном значении сигнала контейнера алгоритм извлечения сообщения должен иметь решение (отсутствие разрывов функции извлечения); алгоритм маскировки должен обеспечивать достаточный уровень сокрытия сигнала (статистический и визуальный); система должна быть защищена ключом, обеспечивающим невозможность обнаружения и извлечения встроенного сообщения без знания ключа.

2. Разработана методология синтеза двухкомпонентных стеганографических систем. Определены три направления реализации двухкомпонентного контейнера: когда каждая компонента представляет собой функцию сигнала пустого контейнера и сигнала сообщения; когда первая компонента является сигналом пустого контейнера, а вторая компонента представляет собой функцию сигналов первой компоненты и сообщения; когда каждая компонента представляет собой функцию двух информативных сигналов. Три рассмотренных направления объединяются свойством инвариантности. Вторые два направления являются модификациями первого направления и позволяют получить новые свойства (скрыть факт встраивания первой

компоненты, и обеспечить извлечение обоих сигналов в случае взаимной маскировки) и реализовать новые стеганографические методы, как в условиях ограничения разрядности представления данных (второе направление), так и в системах, где требуется восстановление маскирующего и маскируемого сигнала (третье направление).

3. Разработан способ формирования двухкомпонентного контейнера, встраиваемого в покрывающий объект и обладающий следующими преимуществами:

- повышена эффективность сокрытия информации, выражающаяся в уменьшении дивергенции Кульбака–Лейблера в 4–5 раз (в зависимости от параметров покрывающего объекта) при использовании методов на основе НЗБ;
- совместимость разработанного метода с известными стеганографическими алгоритмами, что позволяет повысить его эффективность (степень сокрытия или пропускную способность). Это достигается за счёт полного сокрытия первой компоненты, так как она принимает значение покрывающего объекта (фактически встраивается только вторая компонента);
- достигнута высокая сложность извлечения сообщения (защита от прочтения и изменения) в случае перемешивания значений первой компоненты. Количество возможных расположений первой компоненты для одного отсчёта равно количеству бит покрывающего объекта.

4. Разработан комплекс математических моделей двухкомпонентных стеганографических систем на основе суммы, произведения и отношения линейных функций двух сигналов. Особенностью математических моделей является использование двух встраиваемых сигналов, каждый из которых является функцией встраиваемого сообщения. Это позволяет формализовать параметры стеганографических систем. В работе исследованы две функции связи встраиваемых сигналов – аддитивная и мультипликативная. Математические модели разработаны для двух направлений встраивания сообщения – когда каждая компонента представляет собой функцию сигнала пустого контейнера и сигнала сообщения и алгоритма, когда каждая компонента контейнера представляет собой функцию двух информативных сигналов.

5. Разработаны способы выбора параметров двухкомпонентных стеганографических систем. Исследованные в работе алгоритмы построены таким образом, чтобы функция извлечения сообщения имела точку разрыва. Если система работает вблизи точки разрыва, то чувствительность к вариации параметров (коэффициентов) позволяет осуществить защиту от вскрытия с помощью секретных (ключевых) коэффициентов. В работе определены условия реализуемости стеганографических систем, условия максимальной чувствительности к вариации коэффициентов, для каждого алгоритма определены ключевые коэффициенты, ошибка в которых приводит к искажению извлекаемого сигнала сообщения. Для нелинейных алгоритмов встраивания определена зависимость смещения точки разрыва от вариации сигнала сообщения или маскирующего сигнала и определены значения сигналов, при которых возникает разрыв функции извлечения

6. Разработаны технические решения двухкомпонентных стеганографических систем в виде структурных схем и их программных реализаций:

- численные модели исследования параметров двухкомпонентных стеганографических систем в среде Mathcad;
- структурные схемы подсистем встраивания сообщения и подсистем извлечения сообщения для всех разработанных алгоритмов, включая алгоритмы с синтезом маскирующего сигнала из сигнала покрывающего объекта, а также структурные схемы подсистем извлечения сообщения с предварительным расчётом коэффициентов;
- имитационные модели алгоритмов встраивания сообщений в растровые изображения «оттенки серого» (8 бит) и типа «RGB» (24 бита) для различных исследованных алгоритмов;
- имитационные модели для данных, имеющих различные виды ограничения разрядности, работающие в реальном времени в среде MATLAB–Simulink;
- имитационные модели встраивания звукового сообщения в звуковой покрывающий сигнал, работающие в реальном времени в среде MATLAB–Simulink.

Полученные результаты позволяют повысить эффективность защиты информации с помощью стеганографических методов за счёт повышения сокрытия (снижение дивергенции Кульбака–Лейблера) и повышения сложности извлечения сообщения (за счёт необходимости поиска первой компоненты). Дальнейшее развитие темы планируется в направлениях:

• исследование других функций формирования компонент. Сюда следует отнести нелинейные функции, позволяющие получить новые свойства стеганографических систем;

• исследование маскировки сообщений случайными сигналами с целью получения заданных статистических характеристик стеганографического контейнера при условии использования чисел с большой разрядностью представления данных;

• использование нелинейных алгоритмов связи встраиваемых сигналов u_1 и u_2. В этом случае анализ двухкомпонентных стеганографических систем значительно осложнится;

• дальнейшее развитие практической стороны внедрения за счёт адаптации двухкомпонентных систем к разным типам контейнеров и комбинации двухкомпонентных контейнеров с известными стеганографическими методами.

СПИСОК ЛИТЕРАТУРЫ / REFERENCES

1. Грибунин В. Г., Оков И. Н., Туринцев И. В. Цифровая стеганография. М.: Солон-Пресс. 2002. [[(In Russian).]]
2. Fridrich J. Steganography in Digital Media. Principles, Algorithms and Applications. Cambridge University Press, 2010.
3. Шакурский В. К., Шакурский М. В. Сжимающие отображения в инвариантных преобразователях и системах стеганографии. Самара: Изд-во СНЦ РАН, 2014. [[Shakursky V. K., Shakursky M. V. Compressive Mappings in Invariant Converters and Steganography Systems. Samara: Publishing House of the SNC RAS, 2014. (In Russian).]]
4. Шакурский М. В. Формирование контейнера для стеганографической системы на основе сжимающих отображений // Радиотехника. 2015. № 2. С. 134-139. [[Shakursky M. V. “Formation of a container for a steganographic system based on compressive mappings” // Radio-technics. 2015. No. 2, pp. 134-139. (In Russian).]]
5. Шакурский М. В., Шакурский В. К. Стеганографическая система на основе сжимающих отображений // Вопросы защиты информации. 2015. № 2. С. 74-78. [[Shakursky M. V., Shakursky V. K. “A steganographic system based on compressive mappings” // Information Security Issues. 2015. No. 2, pp. 74-78. (In Russian).]]
6. Шакурский М. В., Шакурский В. К. Алгоритм сжатия полосы неопределённости в двухканальных инвариантных структурах // Сборник статей I международной заочной научно-технической конференции «Алгоритмические и программные средства в информационных технологиях, радиоэлектронике и телекоммуникациях». Тольятти: Изд-во ПВГУС, 2013. Ч. 2. С. 313-318. [[Shakursky M. V., Shakursky V. K. “Uncertainty band compression algorithm in two-channel invariant structures” // Collection of Articles of the I International Correspondence Scientific and Technical Conference "Algorithmic and Software Tools in Information Technologies, Radio Electronics and Telecommunications". Togliatti: Publishing House of PVGUS, 2013. Part 2, pp. 313-318. (In Russian).]]
7. M. V. Shakurskiy, V. K. Shakurskiy, V. I. Volovach. “Computer model of steganographic system based on contraction mapping with stream audio container” // in: Proceedings of IEEE East-West Design & Test Symposium (EWDTS’2015) / KNURE, Kharkov, 2015, pp. 306-309. [[(In Russian).]]
8. Шакурский М. В. Стеганографическая система на основе сжимающих отображений // Материалы VIII международной научно-технической конференции «Радиолокация и радиосвязь». Москва: ИРЭ им. В. А. Котельникова РАН, 2014. С. 90-93. [[Shakursky M. V. “Steganographic system based on compressive mappings” // In: Proceedings of the VIII International Scientific and Technical Conference "Radiolocation and Radio Communication". Moscow: IRE V. A. Kotelnikov RAS, 2014, pp. 90-93. (In Russian).]]
9. Шакурский М. В. Формирование контейнера для стеганографической системы методом контрольного значения // Сборник статей VII международной заочной научно-технической конференции «Информационные технологии. Радиоэлектроника. Телекоммуникации». Тольятти: Изд-во ПВГУС, 2017. С. 547-550. [[Shakursky M. V. “Formation of a container for a steganographic system by the control value method” // Collection of articles of the VII International Correspondence Scientific and Technical Conference “Information Technologies. Radioelectronics. Telecommunications. Togliatti: Publishing House of PVGUS, 2017. Pp. 547-550. (In Russian).]]
10. Шакурский М. В. Математические модели двухкомпонентных инвариантных стеганографических систем, использующих различные алгоритмы связи встраиваемых сигналов // Вопросы защиты информации. 2018. № 2. С. 3-8. [[Shakursky M. V. “Mathematical models of two-component invariant steganographic systems using various algorithms for connecting embedded signals” // Information Security Issues. 2018. No. 2, pp. 3-8. (In Russian).]]
11. Шакурский М. В., Шакурский В. К. Оценка стойкости стеганографической системы // Успехи современной радиоэлектроники. 2015. № 11. С. 87-91. [[Shakursky M. V., Shakursky V. K. “Evaluation of the stability of a steganographic system” // Advances in Modern Radio Electronics. 2015. No. 11, pp. 87-91. (In Russian).]]
12. M. V. Shakurskiy, V. K. Shakurskiy, V. I. Volovach. “Two-channel real-time steganographic system” // In: Proceedings of IEEE East-West Design & Test Symposium (EWDTS’2014) / KNURE, Kharkov, 2014, pp. 309-311.
13. Шакурский М. В. Свойства инвариантных двухкомпонентных стеганографических систем, использующих аддитивный алгоритм связи встраиваемых сигналов // Вопросы защиты информации. 2018. № 4. С. 3-9. [[Shakursky M. V. “Properties of invariant two-component steganographic systems using an additive algorithm for connecting embedded signals” // Information Security Issues. 2018. No. 4, pp. 3-9. (In Russian).]]

14. Шакурский М. В. Двухкомпонентная стеганографическая система на основе суммы линейных функций двух сигналов, использующая мультипликативный вид связи встраиваемых сигналов // Проблемы информационной безопасности. Компьютерные системы. 2020. № 1 (41). С. 44-49. [[Shakursky M. V. “Two-component steganographic system based on the sum of linear functions of two signals, using a multiplicative type of connection of embedded signals” // Problems of Information Security. Computer Systems. 2020. No. 1 (41), pp. 44-49. (In Russian).]]

15. M. V. Shakurskiy, V. N. Kozlovskiy, V. V. Ermakov, N. A. Konahina, A. N. Grushkin. “Covert communication device for electrotechnical systems based on invariant transform” // in: Reliability, Infocom Technologies and Optimization (Trends and Future Directions) 6th International Conference ICRITO. 2017, pp. 238-242.

16. Шакурский М. В. Двухкомпонентная стеганографическая система на основе суммы линейных функций двух сигналов, использующая аддитивный вид связи встраиваемых сигналов // Вопросы защиты информации. 2020. № 1. С. 10-13. [[Shakursky M. V. “Two-component steganographic system based on the sum of linear functions of two signals, using an additive type of connection of embedded signals” // Information Security Issues. 2020. No. 1, pp. 10-13. (In Russian).]]

17. M. V. Shakurskiy, V. N. Kozlovskiy, A. N. Chekmarev, V. I. Sanchugov. “Invariant algorithm of information concealing for electrotechnical systems” // In: 2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus). 2020. DOI: 10.1109/EIConRus49466. 2020.9039140

18. Шакурский М. В., Шакурский В. К. Устройство сокрытия информации. Пат. 2546307 РФ, МПК H04L 9/00, H04K 3/00; заявл. 10.06.2014. Опубл. 10.04.2015. Бюл. 10. [[Shakursky M.V., Shakursky V.K. “Information concealment device”. Pat. 2546307 RF, IPC H04L 9/00, H04K 3/00; dec. 06/10/2014. Published 04/10/2015. Bull. 10. (In Russian).]]

19. Шакурский М. В., Шакурский В. К. Способ скрытой передачи информации. Пат. 2546306 РФ, МПК H04L 9/00, H04K 3/00; заявл. 10.06.2014. Опубл. 10.04.2015. Бюл. 10. [[Shakursky M. V., Shakursky V. K. “A method of covert transmission of information”. Pat. 2546306 RF, IPC H04L 9/00, H04K 3/00; dec. 06/10/2014. Published 04/10/2015. Bull. 10. (In Russian).]]

20. Шакурский М. В., Козловский В. Н. Выбор ключа в инвариантных двухкомпонентных стеганографических системах, использующих мультипликативный алгоритм связи встраиваемых сигналов // Проблемы информационной безопасности. Компьютерные системы. 2018. № 4. С. 68-73. [[Shakursky M. V., Kozlovsky V. N. “Key selection in invariant two-component steganographic systems using a multiplicative algorithm for connecting embedded signals” // Problems of Information Security. Computer Systems. 2018. No. 4, pp. 68-73. (In Russian).]]

21. Шакурский М. В. Двухкомпонентная стеганографическая система на основе отношения линейных функций двух сигналов, использующая аддитивный вид связи встраиваемых сигналов // Инфокоммуникационные технологии. 2020. № 1. С. 56-61. [[Shakursky M. V. “Two-component steganographic system based on the ratio of linear functions of two signals, using an additive type of connection of embedded signals” // Infocommunication Technologies. 2020. No. 1, pp. 56-61. (In Russian).]]

22. Шакурский М. В. Выбор ключа в двухкомпонентных стеганографических системах, использующих взаимное зашумление компонент // Инфокоммуникационные технологии. 2019. № 2. С. 229-233. [[Shakursky M. V. “Key selection in two-component steganographic systems using mutual component noise” // Infocommunication Technologies. 2019. No. 2, pp. 229-233. (In Russian).]]

23. Шакурский М. В. Устойчивость стеганографической системы на основе сжимающих отображений // Актуальные вопросы развития инновационной деятельности в новом тысячелетии. 2015. № 3 (14). С. 51-54. [[Shakursky M. V. “Stability of a steganographic system based on compressive mappings” // Topical Issues of Innovation Development in the New Millennium. 2015. No. 3 (14), pp. 51-54. (In Russian).]]

24. Козловский В. Н., Шакурский М. В., Газизулина А. Ю., Диденко Н. И., Крыльцов С. Б. Инвариантный алгоритм сокрытия информации для электротехнических систем // Материалы Международной конференция по мягким вычислениям и измерениям / Санкт-Петербургский государственный электротехнический университет "ЛЭТИ" им. В. И. Ульянова (Ленина), 2018. С. 134-137. [[Kozlovsky V. N., Shakursky M. V., Gazizulina A. Yu., Didenko N. I., Kryltsov S. B. “Invariant algorithm for hiding information for electrical systems” // In: Proceedings of the International Conference on Soft Computing and Measurement / Saint-Petersburg State Electrotechnical University "LETI" them. V. I. Ulyanova (Lenin), 2018, pp. 134-137. (In Russian).]]

25. Шакурский М. В., Шакурский В. К. Двухканальная система сокрытия информации с взаимным зашумлением каналов // Радиотехника. 2016. № 2. С. 96-99. [[Shakursky M. V., Shakursky V. K. “Two-channel information concealment system with mutual channel noise” // Radiotechnics. 2016. No. 2, pp. 96-99. (In Russian).]]

26. Шакурский М. В. Устройство сокрытия информации. Пат. 167074 РФ, МПК H04L 9/00, H04K 3/00; заявл. 28.01.2016. 20.12.2016. Бюл. 35. [[Shakursky M.V. “Information concealment device”. Pat. 167074 RF, IPC H04L 9/00, H04K 3/00; dec. 01/28/2016. 12/20/2016. Bull. 35. (In Russian).]]

27. Шакурский В. К., Шакурский М.В., Козловский В. Н., Сорокин А. Г. Устройство сокрытия информации. Пат. 174362 РФ, МПК H04L 9/00, H04K 3/00, G06F 21/00; заявл. 23.03.2017. 11.10.2017. Бюл. 29. [[Shakursky V.K., Shakursky M.V., Kozlovsky V.N., Sorokin A.G. “Information concealment device”. Pat. 174362 RF, IPC H04L 9/00, H04K 3/00, G06F 21/00; dec. 03/23/2017. 10/11/2017. Bull. 29. (In Russian).]]

28. Шакурский М. В., Шакурский В. К. Компьютерное моделирование стеганографической системы основанной на сжимающих отображениях // Инновации в науке: применение и результаты. 2014. № 9. С. 34-37. [[Shakursky M. V., Shakursky V. K. “Computer modeling of a steganographic system based on compressive mappings” // Innovations in Science: Application and Results. 2014. No. 9, pp. 34-37. (In Russian).]]

29. Шакурский М. В. Численное моделирование стеганографической системы, построенной на основе сжимающих отображений для звукового сигнала // Сборник статей девятой международной научно-практической конференции «Наука промышленности и сервису». Тольятти: Изд-во ПВГУС, 2014. С. 293-298. [[Shakursky M. V. “Numerical modeling of a steganographic system built on the basis of compressive mappings for an audio signal” // In: Collection of articles of the ninth international scientific and practical conference "Science of Industry and Service". Tolyatti: PVGUS Publishing House, 2014, pp. 293-298. (In Russian).]]

30. Шакурский М. В. Двухкомпонентная стеганографическая система встраивания информации в звуковой сигнал, работающая в реальном времени // Проблемы информационной безопасности. Компьютерные системы. 2020. № 2. С. 40-45.

[[Shakursky M. V. “Two-component steganographic system for embedding information into an audio signal, working in real time” // Problems of Information Security. Computer Systems. 2020. No. 2, pp. 40-45. (In Russian).]]

31. Шакурский М. В. Метод встраивания информации в младшие биты растровых изображений без сжатия, использующий двухкомпонентный контейнер // Вопросы защиты информации. 2020. № 2. С. 3-7. [[Shakursky M. V. “A method of embedding information into the least significant bits of raster images without compression, using a two-component container” // Information Security Issues. 2020. No. 2, pp. 3-7. (In Russian).]]

32. Шакурский М. В. Алгоритм сокрытия использования двухкомпонентного контейнера в стеганографической системе // Вопросы защиты информации. 2020. № 3. С. 3-5. [[Shakursky M.V. “Algorithm for concealing the use of a two-component container in a steganographic system” // Issues of Information Security. 2020. No. 3, pp. 3-5. (In Russian).]]

33. Шакурский М. В., Шакурский В. К. Стеганографический контейнер на основе симметричных изображений // Сборник статей V международной заочной научно-технической конференции «Информационные технологии. Радиоэлектроника. Телекоммуникации». Тольятти: Изд-во ПВГУС, 2015. Ч. 2. С. 270-275. [[Shakursky M. V., Shakursky V. K. “Steganographic container based on symmetrical images” // Collection of articles of the V International Correspondence Scientific and Technical Conference “Information Technologies. Radioelectronics. Telecommunications”. Tolyatti: Publishing House of PVGUS, 2015. Part 2, pp. 270-275. (In Russian).]]

34. Шакурский М. В. Алгоритм стеганографического преобразования для растрового изображения // Сборник статей V международной заочной научно-технической конференции «Информационные технологии. Радиоэлектроника. Телекоммуникации». Тольятти: Изд-во ПВГУС, 2015. Ч. 2. С. 276-281. [[Shakursky M. V. “Steganographic transformation algorithm for a bitmap image” // Collection of articles of the V International Correspondence Scientific and Technical Conference “Information Technologies. Radioelectronics. Telecommunications”. Tolyatti: Publishing House of PVGUS, 2015. Part 2, pp. 276-281. (In Russian).]]

Поступила в редакцию 11 августа 2023 г.

МЕТАДАННЫЕ / METADATA

Title: Invariant systems of steganographic information protection in real time using two-component containers.

Abstract: The article presents an overview of the results of the study of invariant systems of steganographic information protection in real time. The object of research is information security systems using steganographic technologies. The subject of the study is two-component systems of steganographic information protection, which ensure the invariance of algorithms for extracting a message from a masking signal and are highly sensitive to variations in the key coefficients of the algorithm. The goal is to improve the efficiency of steganographic information protection using two-component containers built based on two signal transformations and the use of message extraction functions in the break area. To achieve the goal, the following have been developed: 1) the scientific and practical concept of an invariant steganographic system; 2) methodology for the implementation of a two-component steganographic container; 3) a method of embedding a two-component container in a covering object; 4) a complex of mathematical models of subsystems for embedding a message signal in a two-component container and subsystems for extracting a message signal from a two-component container; 5) methods for choosing the parameters of two-component steganographic algorithms that provide a high level of information hiding and resistance to hacking; 6) technical solutions for two-component steganographic systems based on the results of numerical and simulation modeling and software of the proposed two-component steganographic information security systems. The methods of mathematical and numerical modeling, system analysis, the theory of sensitivity of dynamic systems, the method of spectral analysis, statistical methods, digital signal processing were used.

Key words: steganography; real-time systems; two-component container.

Язык статьи / Language: русский / Russian.

Об авторах / About the authors:

ШАКУРСКИЙ Максим Викторович
ФГБОУ ВО «Поволжский государственный университет телекоммуникаций и информатики», Россия.
Зав. каф. информационной безопасности. Дипл. инж. (Тольят. гос. ун-т, 2004). Д-р техн. наук по метод. и сист. защиты информац., информ. безоп. (Уфимск. гос. авиац. техн ун-т, 2022). Иссл. в обл. цифровой обработки сигналов и стеганографии.
E-mail: m.shakurskiy@gmail.com
ORCID: https://orcid.org/0000-0003-2393-9603
URL: https://elibrary.ru/author_profile.asp?id=649022

SHAKURSKIY Maxim Victorovich
Povolzhskiy State University of Telecommunications and Informatics, Russia.
Head., Dept. of Informational security. Dipl. engineer (Togliatti state university, 2004). Dr. of Tech. Sci. on methods and systems of information security (2022). Research: digital signal processing and steganography.
E-mail: m.shakurskiy@gmail.com
ORCID: https://orcid.org/0000-0003-2393-9603
URL: https://elibrary.ru/author_profile.asp?id=649022

ШАМШАЕВ Максим Юрьевич
ФГБОУ ВО «Поволжский государственный университет телекоммуникаций и информатики», Россия.
Магистрант направления Информационная безопасность.
E-mail: maxsham2000@mail.ru

SHAMSHAEV Maxim Yurievich
Povolzhskiy State University of Telecommunications and Informatics, Russia.
Magister’s degree student of Information Security.
E-mail: maxsham2000@mail.ru