УДК 004.056.5

М.А. Козина

СТЕГАНОГРАФИЧЕСКИЙ МЕТОД ОРГАНИЗАЦИИ СКРЫТОГО КАНАЛА СВЯЗИ, ОСУЩЕСТВЛЯЮЩИЙ ПРОВЕРКУ ЦЕЛОСТНОСТИ ПЕРЕДАВАЕМОЙ ИНФОРМАЦИИ

В работе предложен стеганографический метод, одновременно обеспечивающий скрытую передачу произвольной бинарной последовательности, проверку нарушения целостности дополнительной информации, соблюдение надежности восприятия стеганосообщения, устойчивость к возмущающим воздействиям в канале связи. Основой соответствующего стеганографического алгоритма является предлагаемый способ обеспечения принадлежности коэффициентов преобразования Фурье множеству целых чисел.

Ключевые слова: *стеганографический метод, целостность, дискретное преобразование Фурье, цифровое изображение.*

У роботі запропоновано стеганографічний метод, який одночасно забезпечує приховану передачу довільної бінарної послідовності, перевірку порушення цілісності додаткової інформації, дотримання надійності сприйняття стеганоповідомлення, стійкість до збурних дій в каналі зв'язку. Основою відповідного стеганографічного алгоритму є запропонований спосіб забезпечення приналежності коефіцієнтів перетворення Фур'є до множини цілих чисел.

Ключові слова: *стеганографічний метод, цілісність, дискретне перетворення Фур'є, цифрове зображення.*

The paper presents a steganographic method, which provides secure communication random binary sequence, checking the integrity of violations of the covered information, the compliance of the reliability of the perception of steganographic message, the resistance to disturbing influences in the communication channel. The basis of the relevant steganographic algorithm is a way of providing supplies of Fourier transformation coefficients to the set of integers.

Keywords: *steganography method, integrity, discrete Fourier transformation, digital image.*

Введение

Перспективным направлением в обеспечении безопасности информации в современных системах и сетях является цифровая стеганография [1–3].

В рамках стеганографии дополнительная информация (ДИ) встраивается в не привлекающий внимание объект – основное сообщение, или контейнер, результатом чего является стеганосообщение (СС), которое далее открыто передается адресату по каналу связи либо хранится в таком виде.

Можно выделить две причины широкого распространения научных исследований современности в сфере стеганографии, такие как [4]:

– проблемы защиты прав собственности на информацию, которая представлена в цифровом формате;

– ограничение на использование криптосредств в ряде стран мира.

Первая причина послужила толчком развития стеганографии в области цифровых водяных знаков (ЦВЗ) [3], вторая привела к углублению и расширению исследований в области сокрытия факта передачи ДИ.

Компьютерные технологии придали новый импульс развитию и совершенствованию стеганографии. Сегодня скрытая передача данных и организация проверки целостности ДИ являются важнейшими задачами для различных сфер деятельности человека, которые должны решаться одновременно. Однако существующие стеганографические методы (СМ), осуществляющие решение упомянутой двуединой задачи, не лишены значительных недостатков [5–7], требуют дальнейшей разработки, оставляя рассматриваемую задачу *актуальной*.

С бурным развитием компьютерных технологий к современным СМ предъявляется обязательное требование устойчивости к возмущающим воздействиям в канале связи. Метод пересылки и декодирования ДИ, применяемый в области компьютерной стеганографии, будем называть устойчивым, если формируемое при помощи этого СМ стеганосообщение является нечувствительным (малочувствительным) к возмущающим воздействиям.

С учетом того, что стеганографические методы считаются более устойчивыми к различным видам искажений, если сокрытие ДИ происходит в частотной области [3], в [8] автором настоящей работы предложен СМ, который основан на погружении конфиденциальной информации в частотную область контейнера, в качестве которого выступает цифровое изображение в градациях серого, обеспечивающий скрытую передачу данных в канале общего пользования и проверку целостности встраиваемой ДИ. Переход из пространственной в частотную область изображения происходит с использованием дискретного преобразования Фурье (ДПФ). Матрица частотных коэффициентов строится для блоков нестандартного разбиения исходной матрицы ЦИ. За счет выбора блока разбиения размером 2×2 частотные коэффициенты не содержат мнимой части. Предлагаемая в [8] теоретическая база СМ взята автором за основу нового устойчивого СМ, представленного в данной работе, решающего двуединую задачу, определенную выше.

Цель статьи и постановка исследований

Целью работы является разработка нового СМ, позволяющего обеспечивать скрытую передачу произвольной бинарной последовательности с соблюдением надежности восприятия стеганосообщения, проверку целостности дополнительной информации.

Для достижения поставленной цели в работе решаются следующие *задачи*:

1. Выбор размера блока разбиения матрицы ЦИ, позволяющий получить вещественные, целые коэффициенты ДПФ;

2. Обеспечение решения задачи проверки целостности ДИ с учетом специфики полученных коэффициентов ДПФ;

3. Обеспечение устойчивости разработанного стеганографического алгоритма (СА) к возмущающим воздействиям в канале связи.

Основная часть

В качестве контейнера в работе рассматривается цифровое изображение (ЦИ). Формальным представлением ЦИ является матрица значений яркости пикселей. Известно, что человек обычно не способен заметить изменение в наименьшем значащем бите (НЗБ) значения яркости [4], который фактически является шумом. Поэтому НЗБ можно использовать для встраивания дополнительной информации, обеспечивая при этом ее значительный объем: до $\frac{3}{8}$ объема контейнера (для цветных ЦИ). Это важное свойство используется в одном из самых распространенных на сегодняшний день стеганометодов – методе модификации НЗБ (LSB), к достоинствам которого помимо упомянутого следует отнести простоту использования и организации процесса стеганопреобразования и декодирования ДИ, а к недостаткам – неустойчивость к возмущающим воздействиям, даже незначительным. Предлагаемый в настоящей работе СМ учитывает недостатки метода LSB, хотя использует его как составную часть.

Пусть R – $M\times N$-матрица – одна из цветовых составляющих цветного ЦИ - контейнера произвольного формата, для хранения которого использована схема RGB [9]. Не ограничивая общности рассуждений, все последующие преобразования ЦИ формально будут представляться как преобразования R.

Разобьем матрицу R на непересекающиеся блоки f, размером 2×2. Выполним предварительное кодирование в пространственной области изображения. Для решения задачи 2 корректируется (если необходимо) один из пространственных коэффициентов. Для этого определяется количество четных и нечетных пространственных коэффициентов в блоке. Ничего не следует делать в случае, если их количество совпадает или блок состоит исключительно из всех четных (нечетных) коэффициентов. Иначе необходимо изменить один из пространственных коэффициентов блока. Это возможно сделать одним из предложенных ниже способов: в соответствии с (1) или с (2):

$$if\ (k=1\|k=3)\begin{cases} if\ \mathrm{mod}(f(i,j),2)=0,\ f(i,j)=f(i,j)+1 \\ if\ \mathrm{mod}(f(i,j),2)=1,\ f(i,j)=f(i,j)-1 \end{cases} \quad (1)$$

где k – количество четных элементов исходного блока, $f(i, j)$ – некоторый произвольный элемент блока, ‖ – оператор логического ИЛИ, операция mod – остаток от деления на число Matlab(2009);

$$if\ \mathrm{mod}(\sum_{i=0}^{1}\sum_{j=0}^{1} f(i,j),2)=1,\ f(i,j)=f(i,j)-1, \quad (2)$$

где $f(i, j)$ – некоторый произвольный элемент блока.

Для каждого блока f после преобразования (1) (или (2)), применяется прямое дискретное преобразование Фурье (ПДПФ) (3), в результате которого получается блок F частотных коэффициентов:

$$F(u,v)=\frac{1}{2}\sum_{x=0}^{1}\sum_{y=0}^{1} f(x,y)e^{-i2\pi(\frac{ux}{2}+\frac{vy}{2})} \quad (3)$$

где x, y – индексы элементов блока матрицы контейнера f, $f(x, y)$ – элемент исходного блока; $u = \overline{0,1}$, $v = \overline{0,1}$ – индексы элементов матрицы частотных коэффициентов после применения ПДПФ, $F(u,v)$ – частотный коэффициент.

Благодаря выбору размера 2×2 блока разбиения, а также предварительному корректированию значений элементов блока в пространственной области получаем целые вещественные значения частотных коэффициентов Фурье [8], указанные свойства которых при декодировании будут использованы для проверки целостности ДИ.

ДИ представляется в виде бинарной матрицы размером $\left[\frac{M}{2}\right]\times\left[\frac{N}{2}\right]$,([•] – целая часть аргумента).

Предлагается проводить погружение ДИ (с учетом того, что частотные коэффициенты имеют целые значения) путем замены бита каждого частотного коэффициента $F(i,j)$, $i, j = \overline{0,1}$, очередного используемого для стеганопреобразования блока, стоящего в позиции от правого конца, где $pos \in \{2,3,4\}$, на значение погружаемого бита p. Результатом является блок FF возмущенных частотных коэффициентов с элементами $FF(i,j)$, $i, j = \overline{0,1}$. Таким образом, в 1 блок контейнера погружается 1 бит p ДИ в соответствии с (4):

$$FF(i,j) = bitset(F(i,j), pos, p), \quad i, j = \overline{0,1} \tag{4}$$

где *bitset* – операция, реализованная в среде в Matlab (2009), которая устанавливает нужное значение в указанной позиции значения $F(i,j)$. Такое стеганопреобразование очевидно обеспечит бульшую устойчивость по сравнению с аналогичным алгоритмом внедрения ДИ в НЗБ, при этом, как показал эксперимент, не нарушая надежность восприятия цветного цифрового изображения. Каждое значение частотного коэффициента в области ПДПФ может увеличиться/уменьшиться на 2^1, 2^2 или 2^3, что не вызовет появления видимых артефактов в пространственной области стеганосообщения.

После предлагаемой организации внедрения ДИ все частотные коэффициенты остаются целыми, не меняя своей четности/нечетности. Таким образом, возвращение в пространственную область матрицы осуществиться без округлений (если не учитывать принципиально возможный выход значений яркости пикселей за границы диапазона [0,255]).

Возвращение в пространственную область изображения происходит путем обратного дискретного преобразования Фурье (ОДПФ) (5) для блоков матрицы:

$$ff(x,y) = \frac{1}{2}\sum_{u=0}^{1}\sum_{v=0}^{1} FF(u,v)\, e^{2\pi i\left(\frac{ux}{2}+\frac{vy}{2}\right)} \tag{5}$$

где $x = \overline{0,1}$, $y = \overline{0,1}$ – индексы элементов блока матрицы СС в пространственной области, $ff(x, y)$ – элемент блока ff СС после применения обратного преобразования Фурье.

Декодирование ДИ проводится в несколько этапов.

На первом этапе происходит проверка целостности ДИ, внедренной в цифровое цветное изображение. Для этого из ЦИ-стеганосообщения выделяется

матрица *R*, которая разбивается на непересекающиеся 2×2 − блоки $\overline{ff}$ (которые в общем случае могут отличаться от блоков СС , полученных в результате (5), поскольку СС могло претерпеть возмущающее воздействие), для каждого блока $\overline{ff}$ строится ПДПФ, результатом чего является блок $\overline{F}$. В каждом блоке происходит проверка на принадлежность множеству целых чисел четырех частотных коэффициентов. Если хотя бы в одном блоке, хотя бы для одного частотного коэффициента было получено нецелое значение, то можно говорить о нарушении целостности ДИ (при условии игнорирования возможного выхода значений яркости пикселей за пределы [0, 255] при возвращении в пространственную область изображения после погружения ДИ).

Второй этап осуществляет дополнительную проверку целостности ДИ и ее декодирование.

Декодирование из каждого использованного в процессе стеганопреобразования блока 1 бита ДИ происходит с одновременной проверкой равенства (6):

$$bitget(\overline{F}(0,0), pos) = bitget(\overline{F}(1,0), pos) = bitget(\overline{F}(0,1), pos) = bitget(\overline{F}(1,1), pos) \quad (6)$$

где *bitget* − операция в Matlab (2009), которая выдает значение, стоящее в указанной позицию *pos* для $\overline{F}(i, j)$. В случае невыполнения (6) делается вывод о нарушении целостности ДИ.

В случае, если целостность ДИ не нарушена, то значение очередного бита *p* ДИ получается в соответствии с соотношением:

$$\begin{bmatrix} p = 0, если\ bitget\left(\overline{F}(i, j), pos\right) = 0, \\ p = 1, если\ bitget\left(\overline{F}(i, j), pos\right) = 1 \end{bmatrix} i, j = \overline{0,1} \quad (7)$$

В случае если целостность нарушена, декодирование ДИ происходит с учетом частоты появления 0 и 1 в $bitget\left(\overline{F}(i, j), pos\right)$, $i, j = \overline{0,1}$. Если количество 0 и 1 для очередного блока СС совпадает, то очередной бит ДИ не определен.

Результаты

Исходя из всего вышесказанного, основные шаги предлагаемого стеганографического метода, осуществляющего организацию скрытого канала связи с одновременной проверкой целостности ДИ, выглядят следующим образом.

Погружение ДИ:

1. Одна из матриц цветного ЦИ − контейнера *R* разбивается на непересекающиеся блоки *f* размера 2×2.

2. Для каждого блока *f* ЦИ-контейнера, используемого в процессе стеганопреобразования:

2.1. Проводится корректировка (если необходимо) значений яркости пространственных коэффициентов по формуле (1) или (2);

2.2. Осуществляется переход в частотную область при помощи ПДПФ (3). Результат − блок *F*;

2.3. В частотные коэффициенты блока *F* происходит погружение 1 бита ДИ (4). Результат − блок *FF*;

2.4. Перевод блока *FF* в пространственную область в соответствии с (5). Результат – блок *ff* стеганосообщения.

Декодирование ДИ:

1. Одна из матриц цветного ЦИ-стеганосообщения $\overline{R}$ разбивается на непересекающиеся блоки ff размера 2×2.

2. Для каждого блока ff ЦИ-стеганосообщения, используемого в процессе декодирования:

2.1. Осуществляется переход в частотную область при помощи ПДПФ (3). Результат – блок $\overline{F}$;

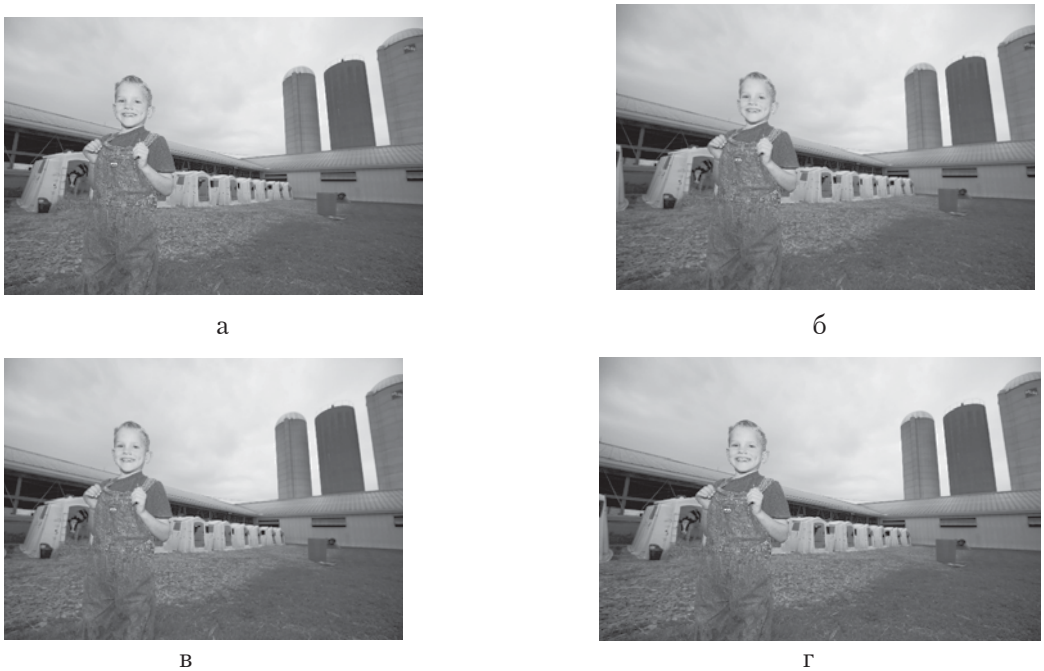
2.2. Проверка целостности внедренной ДИ:

2.2.1. Если среди $\overline{F}(i, j)$, $i, j = 0,1$, существует $\overline{F}(i, j) \notin Z$, где Z – множество целых чисел, то целостность ДИ нарушена;

2.2.2. Дополнительная проверка целостности в соответствии с (6).

2.3. Декодирование бита ДИ в соответствии с (7).

Для разработанного стеганографического метода путем представительного вычислительного эксперимента была проведена проверка соблюдения надежности восприятия получаемого стеганосообщения. Проверка проводилась двумя способами: путем субъективного ранжирования; стандартным образом – при помощи оценки величины пикового отношения "сигнал-шум" *PSNR*. В ходе проверки были задействованы 500 цветных ЦИ, разных по жанру, контрастности, цветности, яркости (экспериментальное множество (ЭМ)). Артефакты на изображениях-стеганосообщениях при визуальном анализе обнаружены не были (типичный пример, подтверждающий сказанное, представлен на рис.1). Среднее значение *PSNR* при использовании разных значений $pos \in \{2,3,4\}$ при внедрении ДИ составило 42 dB, что считается приемлемым с точки зрения оценки визуального качества стеганосообщения [2].



а б в г

Рис. 1. Результаты стеганопреобразования разработанным стеганометодом: а – изображение-контейнер; б – СС, сформированное для pos=2; в – СС, сформированное для pos=3; г – СС, сформированное для pos=4.

Тестирование работы предложенного стеганометода осуществлялось в условиях отсутствия каких-либо возмущающих воздействий на СС (целостность ДИ здесь была подтверждена в 100 % задействованных ЦИ из ЭМ), а также в условиях активных атакующих действий на СС, которые, с учетом того, что в результате любых атак на СС должна сохраняться его надежность восприятия (в противном случае все действия атакующего будут без труда обнаружены сторонами, организующими скрытый канал связи), моделировались при помощи малых возмущающих воздействий.

Эффективность декодирования ДИ в разработанном стеганографическом методе оценивалась в соответствии с формулой:

$$P = \frac{Количество\ бит\ ДИ, восстановленных\ верно}{Общее\ количество\ бит\ ДИ} \cdot 100\%$$

Для проверки устойчивости СМ после внедрения ДИ на СС, полученные на основе ЦИ из ЭМ, накладывались шумы с различными параметрами (гауссовский и мультипликативный; результаты декодирования ДИ представлены в табл. 1, 2), проводилось сжатие СС (jpeg) (табл. 3). Нарушение целостности ДИ разработанным СМ было зафиксировано в 100% тестируемых изображений.

Таблица 1

Эффективность *P* декодирования ДИ в разработанном СМ в зависимости от позиции внедрения (pos) в условиях наложения на СС гауссовского шума с нулевым матожиданием и дисперсией σ^2 (%)

pos \ σ^2	0,0001	0,00001
2	51	75.5
3	70	97
4	90	98.9

Таблица 2

Эффективность *P* декодирования ДИ в разработанном СМ в зависимости от позиции внедрения (pos) после наложения мультипликативного шума с дисперсией σ^2, (%)

pos \ σ^2	0,0001	0,00001
2	56	83
3	85	98.5
4	92	99

Анализируя полученные результаты, можно отметить, что при увеличении номера позиции бита, в который внедряется бит ДИ, эффективность *P* декодирования ДИ в разработанном СМ в условиях возмущающих воздействий возрастает. Таким образом, самым оптимальным выбором будет внедрение информации в 4 бит двоичного представления частотных коэффициентов преобразования Фурье.

Таблица 3

Эффективность *P* декодирования ДИ в разработанном СМ в зависимости от выбора коэффициента сжатия (k), а также позиции внедрения (pos) бита ДИ

pos \ k	90 %	100 %
2	56	83
3	85	98.5
4	92	99

Выводы

В работе разработан стеганографический метод, обеспечивающий скрытую передачу произвольной бинарной последовательности с соблюдением надежности восприятия стеганосообщения, осуществляющий проверку целостности дополнительной информации.

В ходе разработки обоснован выбор размера блока матрицы ЦИ-контейнера, используемого при стеганопреобразовании: размер блока 2×2 пикселя позволил обеспечить не только отсутствие мнимой части в значениях коэффициентов дискретного преобразования Фурье, но и отсутствие дробной части, что дало возможность для решения задачи проверки целостности ДИ.

В настоящий момент усилия автора направлены на повышение устойчивости СМ к возмущающим воздействиям.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Стеганография, цифровые водяные знаки и стеганоанализ / А.В. Аграновский, А.В. Балакин, В.Г. Грибунин, С.А. Сапожников. – М. : Вузовская книга, 2009. – 220 с.

2. *Конахович Г.В.* Компьютерная стеганография. Теория и практика / Г.В. Конахович, А.Ю. Пузыренко. – К. : МК-Пресс, 2006. – 288 с.

3. *Грибунин В.Г.* Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. – М. : Солон-Пресс, 2002. – 272 с.

4. *Скляров Д.В.* Искусство защиты и взлома информации / Д.В. Скляров. – СПб. : БХВ-Питербург, 2004. – 288 с. : ил.

5. *Shih, F.* Watermarking, Steganography, and Forensics [Text] / F. Shih. –New York : CRC Press, 2012. – 424 p.

6. *Глумов Н.И.* Алгоритм встраивания полухрупких цифровых водяных знаков для задач аутентификации изображений и скрытой передачи информации / Н.И. Глумов, В.А. Митекин. – Компьютерная оптика. – 2011. – № 2. – Т. 35. – С. 262–267.

7. *Кобозева А.А.* Стеганографический алгоритм скрытой передачи информации, обеспечивающий аутентификацию контейнера / А.А. Кобозева, А.Д. Шовкун. – Науковий вісник Міжнародного гуманітарного університету. –2012. – № 4. – С. 21–28.

8. *Kozina M.O.* Discrete Fourier transform as a basis for steganography method / M. O. Kozina. – Праці Одеського політехнічного університету. – 2014. – Вип. 2(44). – С. 118–126.

9. NRCS Photo Gallery : United States Department of Agriculture. Washington, USA [Электронный ресурс]. – Режим доступа : http : // photogallery.nrcs.usda.gov.

Отримано 2.11.2014

Рецензент Рибальський О.В., доктор технічних наук, професор.