УДК 621.327:621.391

ДВОЙНАЯ ОБФУСКАЦИЯ ТРАНСФОРМАНТ МАЛОРЕСУРСНОГО СТЕГАНОАЛГОРИТМА

Дмитрий Морозов[1], Михаил Шафоростов[1], Сергей Малахов[1], Вадим Сербин[2]

[1] Харьковский национальный университет имени В.Н. Каразина, пл. Свободы, 4, г. Харьков, 61022, Украина
ikurortnik@gmail.com, m61shaforostov@gmail.com, mailgate@meta.ua

[2] ГП «КБ «Южное», ул. Криворожская, 3, 49008, г. Днипро, Украина
buba75@i.ua

Рецензент: Георгий Кучук, д.т.н., проф., НТУ «ХПИ», ул. Кирпичова, 21, г. Харьков, 61000, Украина.
kuchuk56@mail.ru

Поступила в марте 2018

Аннотация. *Целью статьи является ознакомление с основными процедурами адаптивного малоресурсного алгоритма стеганографической обработки изображений и особенностями создания его экспериментальной программы с поддержкой графического интерфейса (мобильного приложения). Предложенная версия программы ориентирована на удобство ее использования на мобильных платформах под управлением операционной системы (ОС) Android. Разработанный адаптивный алгоритм в ручном и автоматическом режимах, позволяет: - определять текущий статус аппаратного обеспечения (мобильной платформы); - учитывать особенности обрабатываемых данных (типы изображений стеганоконтейнера и стеганоконтента); - корректировать параметры работы основных программных модулей исследовательского стеганоалгоритма (блока первичной обработки входных данных (изображений) и блока специальных преобразований – стеганомодуля). Кроме того, проанализированы и другие параметры обработки изображений, имеющих непосредственное влияние на вычислительную сложность всего алгоритма и качество визуализации изображений контейнеров и стеганоконтента. Рассмотренная версия алгоритма является исследовательской и служит средством обеспечения безопасности персональных данных (в данном случае графической информации) пользователей, прежде всего, мобильных гаджетов. Основные свойства синтезированного алгоритма позволяют классифицировать его, как программное средство обеспечения стеганографической защиты, локализованное для условий внутрикадровой обработки изображений. Представленная версия алгоритма требует его дальнейшего совершенствования и имеет своей главной целью подтвердить правильность выбранных методов обработки данных и стратегии создания пользовательского интерфейса соответствующего мобильного приложения.*

Ключевые слова*: обфускация; кодирование с преобразованием; зональное кодирование; стеганография.*

1 Введение

Известно, что одним из эффективных направлений обеспечения сокрытия факта передачи и хранения информации, является применение различных стеганографических методов [1-3]. В рамках данной работы рассматривается цифровое направление стеганографии, локализованное в области изучения возможностей синтеза малоресурсного алгоритма инкапсуляции статических цифровых полутоновых изображений (далее *стеганоконтента*) в другое статическое цифровое изображение (далее *стеганоконтейнер*).

Сужение области исследований в направлении создания легковесного стеганоалгоритма обусловлено практическим интересом создания соответствующего программного решения с дружественным интерфейсом, ориентированного для использования на различных мобильных устройствах (смартфоны, планшеты и т.п.). Предварительно, такой алгоритм должен обеспечивать адаптацию параметров своей работы к параметрам работы и характеристикам мобильной платформы (в «*автоматическом*» режиме работы) или уведомлять о своих возможностях (в «*интерактивном*» режиме) при обеспечении требуемых характеристик формируемого стеганоконтента в сложившихся условиях ресурсных ограничений гаджета (количество и вычислительная сложность работающих активных приложений/задач, текущая температура, фактический заряд встроенной аккумуляторной батареи (АБ) и т.п.). Под уведомлением своих возможностей следует понимать процесс информирования пользователя гаджета о расчетных параметрах его работы (объем обрабатываемого контента или время обработки) для текущих характеристик обрабатываемых изображений (разрешение изображений и их

количество) при требуемом уровне обеспечиваемой скрытности инкапсулируемого контента.

Снижение общей вычислительной сложности стеганоалгоритма (*особенно при пакетной обработке данных*) имеет своей целью обеспечение условий для его последующего применения в составе программного обеспечения различных мобильных платформ (гаджетов), с присущими им качествами и особенностями: 1 – постоянное изменение текущего уровня заряда встроенной АБ, в том числе изменение паспортных характеристик работы АБ по причине ее износа (старения); 2 - поддержка режима многозадачности при работе с мобильными приложениями; 3 - неравномерность в распределении имеющихся вычислительных ресурсов при относительном «равенстве» доступа к ресурсу бортовой АБ между:

а) используемыми мобильными приложениями *(активными приложениями и задачами выполняемых в фоновом режиме (с приоритетом в обслуживании сервисов реального времени))*;

б) имеющимися аппаратными модулями самого гаджета *(например, модулями беспроводной связи (Wi-Fi или Bluetooth), активация функций «работа с гарнитурой» или «фонарик» и т.п.)*;

4 - изменение параметров функционирования отдельных аппаратных элементов мобильной платформы (например, излучаемой мощности *Wi-Fi* модуля) и активных приложений при достижении контрольных (*предустановленных*) значений разряда АБ.

Применительно к очерченной предметной области, задачу можно сформулировать так: – какой объем стеганоконтента с различной степенью его стойкости к обнаружению и декодированию можно сформировать при разных параметрах/условиях работы гаджета (*тип запущенных приложений, текущее состояние бортовой АБ и т.п.*). Цели таких изысканий очевидны – это автоматическое формирование рекомендованных значений параметров работы стеганоалгоритма (*особенно в режиме пакетной обработки данных*) в зависимости от текущих характеристик работы гаджета или же изменение параметров работы самого устройства для достижения требуемых характеристик (*качества*) формируемого стеганоконтента.

2 Основная часть

Сокрытие в цифровых объектах (в данном случае, полутоновых изображениях) какой-либо дополнительной информации, вызывает некоторые искажения этих объектов-контейнеров [1]. При сбалансированных настройках соответствующего алгоритма обработки, возникающие искажения находятся ниже порога чувствительности среднестатистического человека, и не приводят к визуально заметным изменениям/искажениям этих объектов. Таким образом обеспечивается требуемый баланс между сохранение типовых характеристик используемого графического формата представления данных, а так же количеством и интенсивностью проявления различных артефактов изображений, дающих лишний повод задуматься, собственно, о причине их появления. Однако, в оцифрованных объектах, изначально имеющих аналоговую природу, всегда присутствует шум квантования, а при воспроизведении этих объектов проявляются нелинейные искажения, обусловленные особенностями аппаратной части, что способствует дополнительной маскировке сокрытой информации [2].

В основе рассматриваемого алгоритма сокрытия информации лежит внутрикадровый алгоритм сжатия изображений, основанный на использовании метода кодирования с преобразованием (дискретное косинусное преобразование - ДКП) [4,5]. Использование свойств ДКП позволяет встраивать стеганоконтент (полутоновое изображение - 256 градаций яркости) в матрицу коэффициентов преобразования [6] изображения-контейнера. Процедура инкапсуляции стеганоконтента (коэффициентов преобразования скрываемого изображения), реализуется после проведения селекции коэффициентов преобразования изображения-контейнера [4,7]. Для восстановления исходных изображений выполняется обратное ДКП (ОДКП) [5].

Использование методов кодирования с преобразованием обеспечивает получение матриц спектральных коэффициентов (трансформант), в которых большая часть коэффициентов либо близки, либо равны 0. Кроме того, учет свойств зрения человека [5], позволяет аппроксимировать коэффициенты без заметной потери качества визуализируемых изображений. Для

этого используется специализированный механизм квантования коэффициентов [3].

Следует отметить, что в данном случае использовалась симметричная схема реализации кодирования изображений контейнера и контента, т.е. в обоих случаях размер субблоков изображений был одинаковой размерности. Это несколько сужало диапазон возможных настроечных вариаций стеганоалгоритма, но не меняло сути наблюдаемых процессов. Для описания сути алгоритма достаточно удобно рассматривать его отдельными этапами:

1-й этап – деление на блоки и сглаживание исходных изображений; 2-й этап – формирование серий подобных (*идентичных по содержанию*) блоков исходных изображений; 3-й этап – проведение ДКП (для изображений контейнера и стеганоконтента); 4-й этап – проведение модифицированного зонального отбора коэффициентов [7]; 5-й этап – встраивание и обфускация (внутриблочная и межблочная) коэффициентов ДКП; 6-й этап – результирующая обработка и формирование массива «сжатого» стеганокадра.

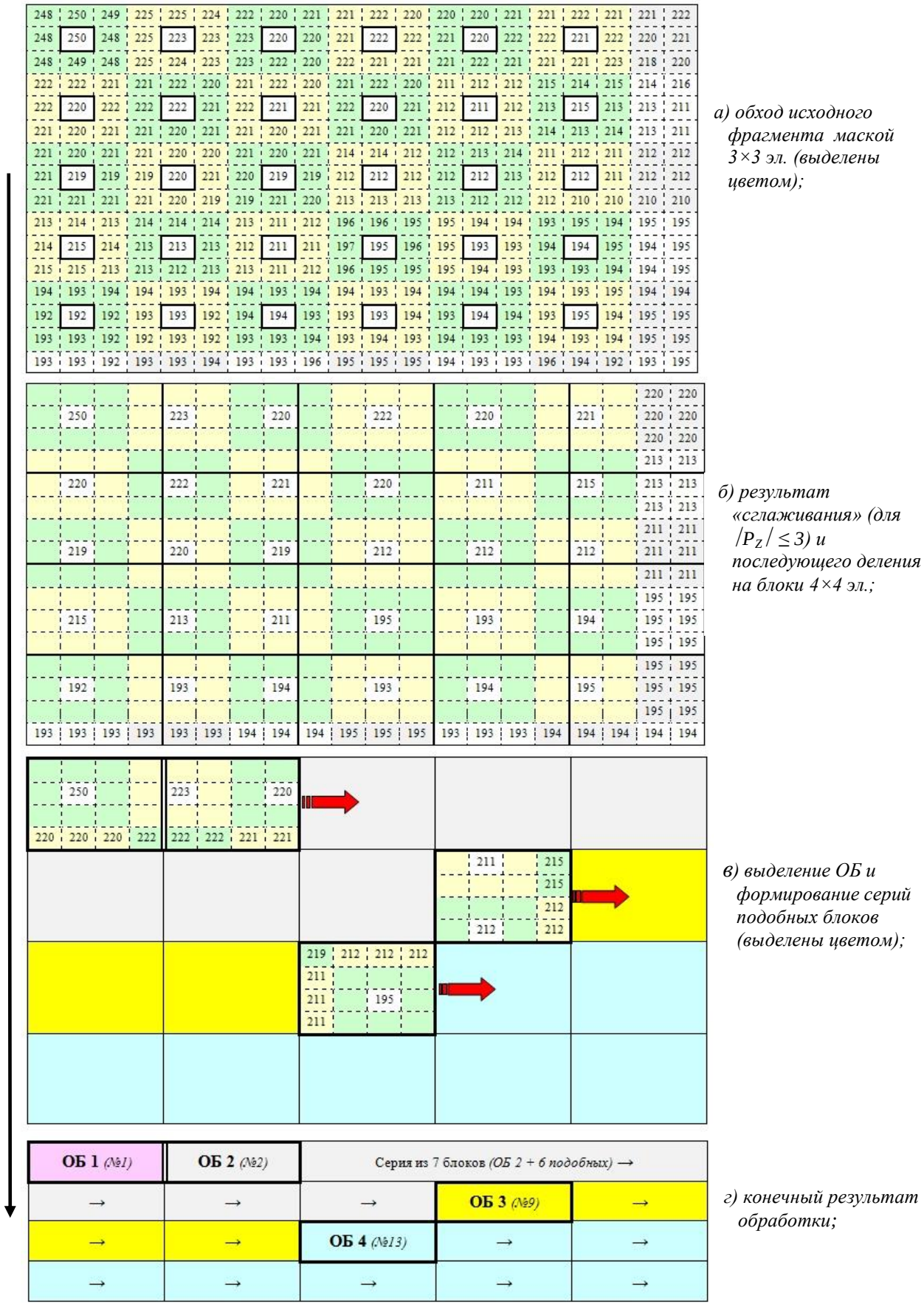
Основной целью 1-го этапа является уменьшение количества визуально не фиксируемых перепадов яркости элементов исходных изображений [5]. Для этого изображения разбиваются на блоки размером 3×3 элемента, после чего в каждом блоке оценивается разница значений центрального элемента с остальными. В случае если полученная разница меньше установленного значения порога загрубления (P_Z), то элемент (пиксел) в этой позиции замещается значением яркости центрального элемента (см. рис.1а). В результате, получаем новые, сглаженные изображения (рис.1б), учитывающие особенности локального распределения яркости элементов исходных изображений для маски 3×3 эл. Этот прием позволяет уменьшить вычислительную сложность всего алгоритма на последующих этапах его работы.

На втором этапе скрываемое изображение делится на блоки установленного размера и в каждом из них определяются элементы с максимальным и минимальным значениями яркости. Далее в соседних блоках изображений (при построчном обходе) эти значения последовательно анализируются и если разности максимальных и минимальных элементов меньше установленного порога загрубления (P_Z), то такие блоки считаются идентичными (*или подобными*), а первый такой блок в серии - опорным блоком (ОБ) (рис.1 в). В результате получаем массив, где указывается порядковый номер каждого ОБ и, соответственно, число его повторов в каждой новой серии (рис.1г). Проведение перечисленных процедур обуславливает необходимость проведения кодирования с преобразованием (в нашем случае ДКП) только для ОБ. Таким образом удается уменьшить общую вычислительную сложность всего алгоритма (*уменьшив его самую ресурсоемкую часть*).

Третий этап представляет собой проведение ДКП над каждым блоком изображения контейнера и ОБ скрываемого контента.

На следующем (4-ом) этапе реализуются процедуры модифицированной зональной селекции коэффициентов преобразования. Вариант маски зонального отбора коэффициентов для блоков размером 8×8 элементов представлен ниже (рис. 2а и 3а). Применение зонального способа отбора исключает необходимость адресации знакомест сохраняемых коэффициентов [4,7] и экономит ресурсы памяти мобильного устройства. Предварительно, для изображения-контейнера сохраняется 10 коэффициентов (рис. 2а), а для улучшения качества восстановления встраиваемых изображений сохраняется несколько большее количество (*в данном случае 14*) коэффициентов преобразования (рис. 3а).

На 5-м этапе производится обфускация коэффициентов ДКП для всех блоков изображений контейнера и контента. Данная процедура выполняется в два этапа с использованием любой из возможных масок обфускации (рис.4,5). В тестовой версии алгоритма соответствующие пары масок перемешивания (для контейнера и контента) строго взаимосвязаны, а их общее количество зависит от размерности используемых блоков. Поскольку позиции коэффициентов не накладываются друг на друга, то полученные после перемешивания массивы совмещаются в одной матрице (рис.4). Размерность субблоков может задаваться вручную и автоматически (*зависит от режима работы алгоритма*), а используемая маска перестановок формируется автоматически, случайным образом. Эти параметры указываются в соответствующей позиции формируемого сжатого файла стеганоконтейнера.



а) обход исходного фрагмента маской 3×3 эл. (выделены цветом);

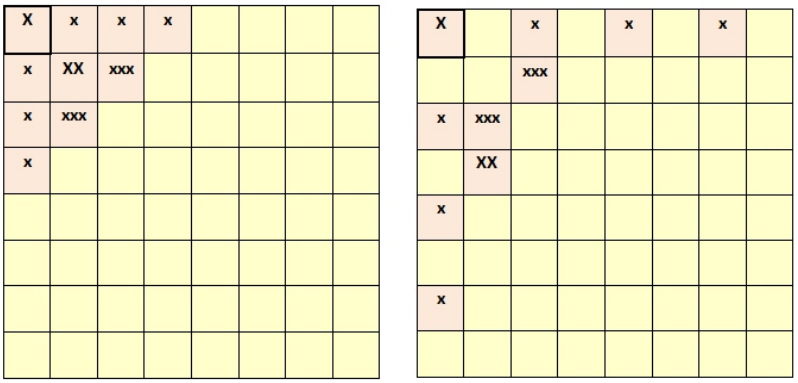
б) результат «сглаживания» (для $|P_Z| \le 3$) и последующего деления на блоки 4×4 эл.;

в) выделение ОБ и формирование серий подобных блоков (выделены цветом);

г) конечный результат обработки;

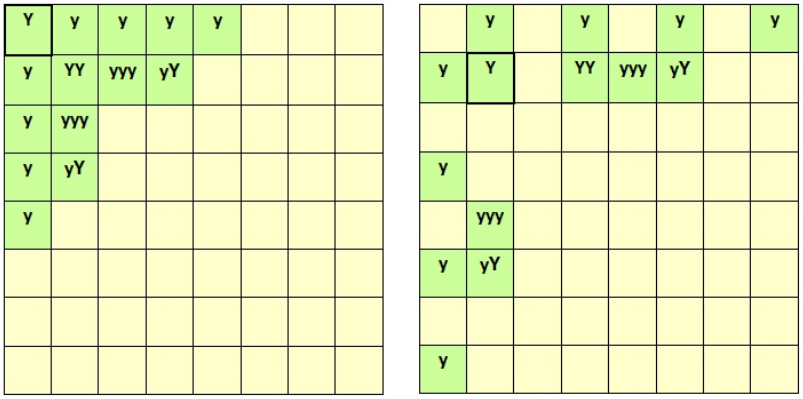
Рис.1 - Формирование серий подобных блоков
(*для блоков размером 4×4 эл.*)

Очевидно, что возможное количество перестановок зависит от размера используемых блоков, поэтому при необходимости увеличить степень скрытности контента (*при неизменном количестве сохраняемых коэффициентов преобразования*), размер блоков увеличивается (*проводится по результатам оценки текущего состояния ресурсов гаджета*).



а) *б)*

Рис. 2 - Маска зонального отбора (*а*) и вариант размещения (*б*) коэффициентов «контейнера»



а) *б)*

Рис. 3 - Маска зонального отбора (*а*) и вариант размещения (*б*) коэффициентов «контента»

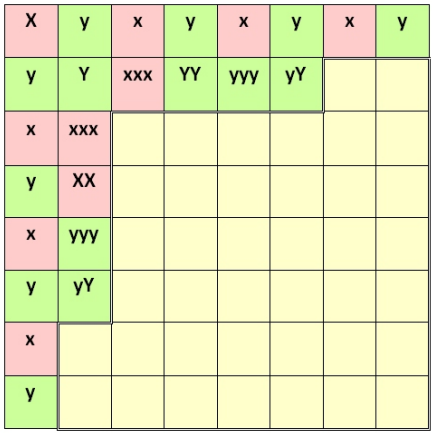


Рис. 4 - Размещения коэффициентов в стеганоконтейнере (*вариант*)

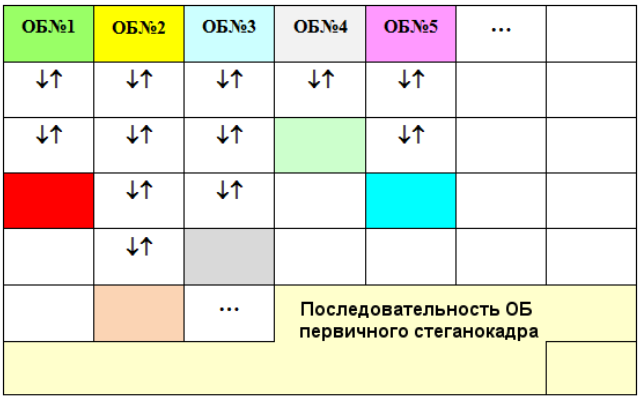
Более того, в ходе экспериментов была проверена идея несимметричной внутриблочной обработки (*размеры субблоков контейнера всегда больше блоков контента*), использование которой значительно затрудняет локализацию элементов инкапсулированного контента и расширяет диапазон возможных перестроек алгоритма. Однако, данный режим обработки несколько сложнее в исполнении и требует введения дополнительных служебных маркеров, позволяющих автоматизировать безошибочное извлечение контента при его декодировании. Результаты такой обработки будут представлены несколько позже.

Для увеличения сложности процедур поиска и извлечения скрытого контента, в исследовательской версии алгоритма, применялся упрощенный механизм межблочной обфускации (*только перемешивание ОБ изображения контейнера* (рис.5)). При этом блоки стеганоконтента встраиваются не последовательно, а в соответствии с генерируемой маской межблочного перемешивания, являющейся еще одним элементом ключа, необходимым для извлечения и последующего декодирования скрытой информации.

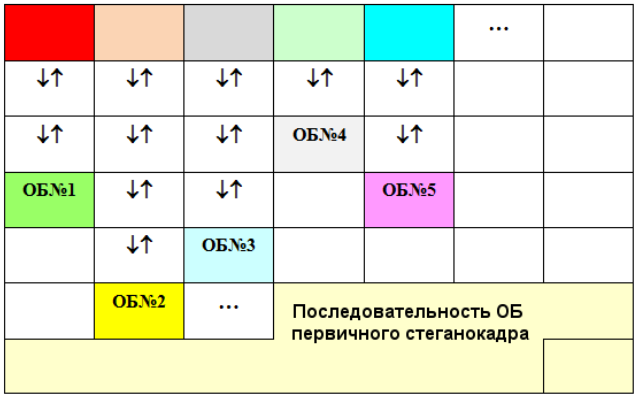
Как и при внутриблочной обработке (обфускации), информация о номере использованного варианта маски межблочного перемешивания, указывается в соответствующей позиции формируемого файла стеганоконтейнера. Очевидно, что использование двухуровневой обфускации стеганоконтента ощутимо расширяет возможности самого алгоритма.

В результате проведения межблочной обфускации формируется первичный стеганокадр. Однако для него присущ один существенный недостаток. После формирования серий подоб-

ных блоков, количество ОБ всегда будет меньше количества блоков изображения-контейнера. Как следствие, может возникнуть ситуация, когда не все блоки контейнера будут «заполнены» информацией стеганоконтента. Так в «рабочих» матрицах - контейнерах предварительно сохраняется 24 коэффициента (рис.4), а в «пустой» матрице только 10 (рис. 2). Это обстоятельство приведет к тому, что при декодировании изображений трудно организовать работу счетчика блоков (матриц-контейнеров). Кроме того, упрощается задача анализа содержимого всего стеганокадра и, как следствие, выявление «заполненных» блоков со всеми вытекающими отсюда последствиями.



а)



б)

Рис. 5 - Исходное (а) и конечное (б) положение матриц-контейнеров до и после проведения межблочной обфускации (*вариант маски*)

Для устранения указанных недостатков необходимо «выровнять» объем цифрового описания всех блока первичного стеганокадра. С этой целью обеспечивается заполнение отсутствующих позиций (в текущем варианте используемой маски) дополнительным балластным содержимым. Для заполнения отсутствующих позиций в тестовой версии алгоритма использовать «родные» значения коэффициентов преобразования, полученные для изображения контейнера. Такой подход имеет двойной эффект: - затрудняет обнаружения аналитиком скрытой информации; - улучшает параметры восстановления исходного изображения контейнера для данной группы блоков.

Последний этап алгоритма предполагает проведение ряда технологических процедур (*в т.ч. характерных и для традиционной реализации алгоритма сжатия JPEG [3,5,8,9]*), таких как уменьшение разрядности и кодирование полученных значений, а также формирование служебного заголовка (ключа) «сжатого» стеганокадра.

Для уменьшения разрядности значений первичного стеганокадра выполняется нормировка значений каждого сохраняемого блока. Исходя из того, что значения яркости исходных изображений варьируются в рамках от 0 до 255, то нормировка значений производится относительно среднего их значения (127) с округлением результата до ближайшего целого.

Учитывая, что все блоки формируемого стеганокадра имеют одинаковый диапазон изменения значений яркости элементов после их нормировки, то обеспечивается возможность синтезировать общий «словарь» для всего стеганокадра. Поэтому дальнейшая кодировка значений первичного стеганокадра обеспечивается применением методов кодирования без потерь информации [5,8,9], например: - методом длин серий или методом Хаффмана.

3 Результаты работы алгоритма

В ходе проведения экспериментов исследовался характер влияния определенных параметров алгоритма на характеристики визуализации изображений и параметров встраивания скрытого контента. Среди таких параметров были использованы следующие: - количество ОБ; - тип изображений контейнера и контента; - размер субблоков изображений (8,16,32); - величина порога загрубления, P_Z (от 1 до 20); - уровень заряда АБ гаджета.

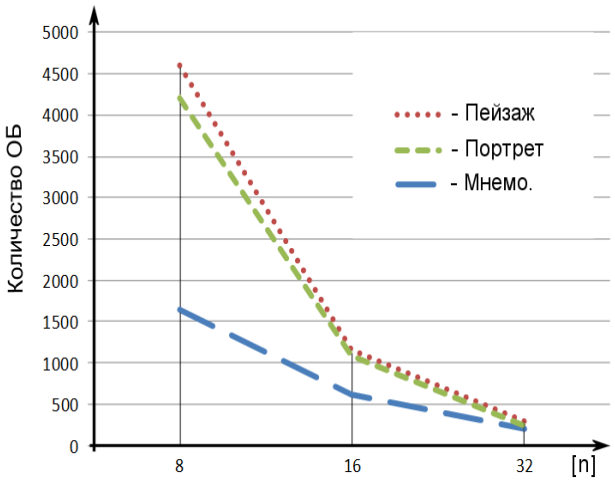
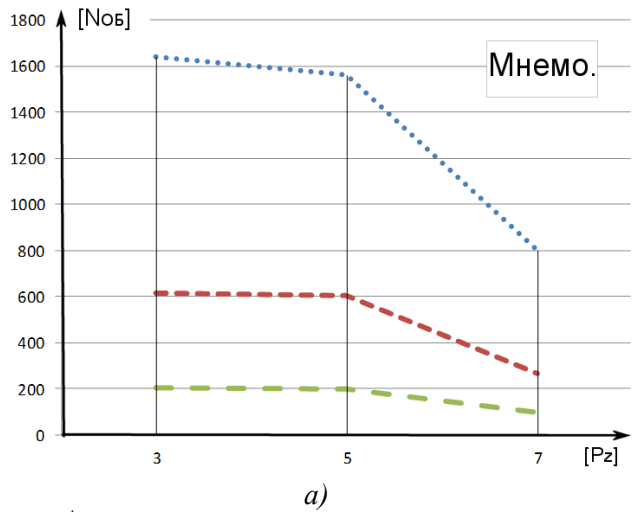


Рис. 6 – Зависимость количества ОБ от n для разных типов изображений

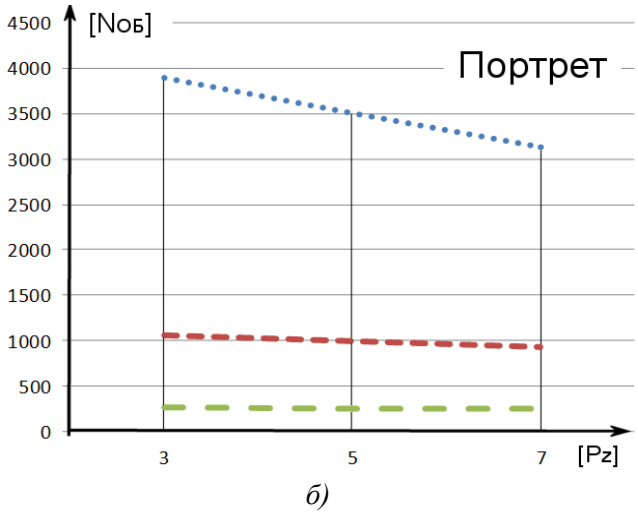
В общем случае количество формируемых ОБ зависит от установленного значения порога загрубления (P_Z). С учетом особенностей восприятия полутоновых изображений [5], характеризующихся различной вероятностью перепада яркости между соседними элементами *(изображения типа мнемосхема, портрет и пейзаж (аэрофотоснимок))*, оптимальный варианты изменения величины P_Z следует ограничить значениями 3,5,7. При таких значениях удается получить наиболее приемлемый баланс между визуальной заметностью проявляющихся искажений и снижением вычислительной сложности алгоритма.

Так на рис. 6 представлены зависимости, отражающие взаимосвязь количества формируемых ОБ с размерностью используемых субблоков (n×n), которые используются при обработке изображений контейнера и контента.

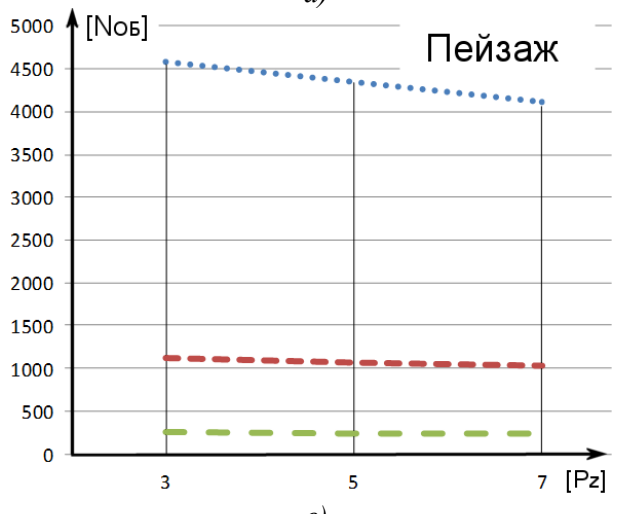
Характер зависимости количества формируемых ОБ ($N_{ОБ}$) от введенного значения P_Z для разных типов изображений (различной вероятности (p) перепада яркости) отображает рис.7.



а)



б)



в)

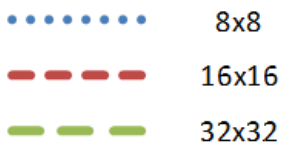
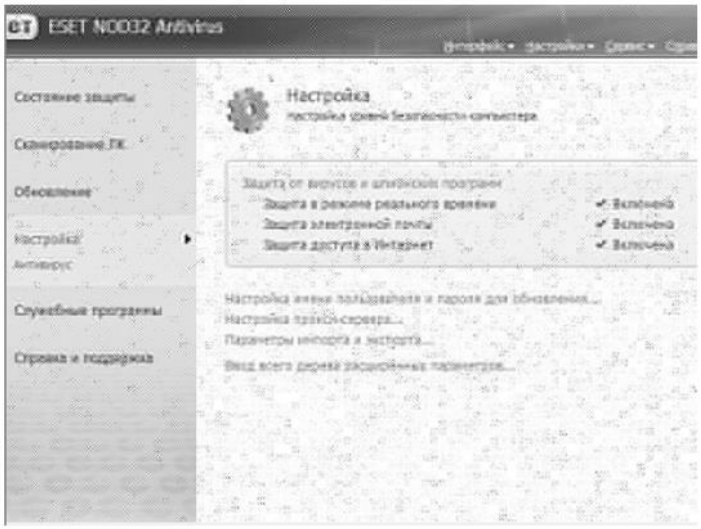


Рис. 7 – Зависимость количества ОБ от P_Z при изменении размерности блоков для различных типов изображений:
а) – мнемосхема *(0,01 ≤ p ≤ 0,03)*;
б) – портрет *(0,03 ≤ p ≤ 0,06)*;
в) – пейзаж/аэрофото *(0,06 ≤ p ≤ 0,1)*.

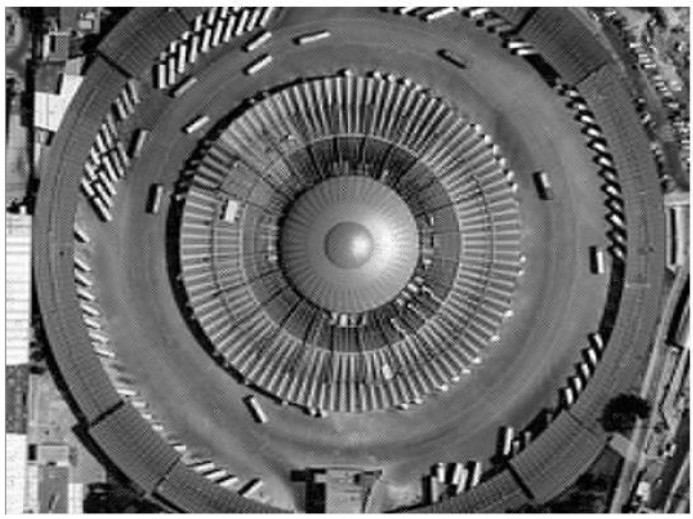
Из анализа представленных результатов следует, что количество формируемых ОБ зависит от 3-х параметров:

- размера субблоков; значения порога загрубления (P_Z); - типа обрабатываемого изображения (*изображений с разной сложностью структуры, т.е. разной вероятностью перепада яркости соседних пикселов*). Так, при увеличении размера субблоков, уменьшается их общее количество в кадре и, соответственно, уменьшается количество ОБ. При увеличении значения P_Z (*при лучших вариантах обработки 3,5,7*) расширяется соответствующий диапазон подобия, поэтому общее количество ОБ уменьшается.

Данные изображения-контента сохраняются в виде значений ОБ, потому от количества инкапсулированных ОБ зависит интенсивность искажений изображения-контейнера. В качестве примера на рис. 8 представлен результат вставки в изображения с разной структурой (*мнемосхема (а) и аэрофотоснимок (б)*) одного и того же изображения (*одинаковое количество ОБ*) с высокой вероятностью перепада яркости соседних элементов (*типа пейзаж*).



а) фрагмент рабочего окна одной из программ;



б) аэрофотоснимок автовокзала в Мехико.

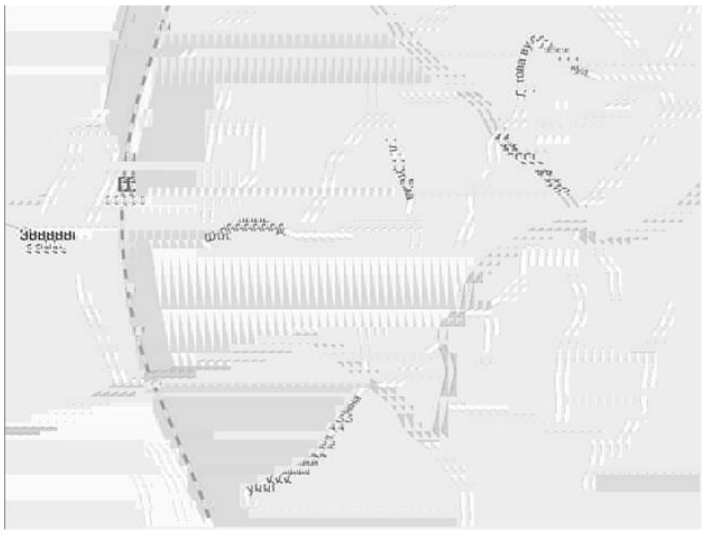
Рис. 8 – Результаты стегановставки
(n=8; P_Z *=3; ОБ 4608)*
в контейнеры с разной вероятностью перепада яркости соседних элементов

Как следует из приведенного примера, при увеличении количества ОБ, в процессе вставки контента в контейнер с простой структурой, визуально увеличиваются искажения изображения-контейнера (*особенно на однородных областях с низкой детальностью фрагментов*), что демаскирует результаты инкапсуляции стеганоконтента. Напротив, результат подобной вставки в изображения со сложной структурой, практически не демаскируется.

Очевидно, что при инкапсуляции изображений с различным количеством ОБ, в изображение контейнер со сложной структурой (*большой вероятностью перепада яркости*), интенсивность визуально фиксируемых искажений контейнера крайне незначительна.

По результатам экспериментального моделирования следует отметить следующее: 1 - при стегановставке изображений с более сложной структурой, чем сам контейнер, наблюдаются интенсивные артефакты, в отличие от случаев инкапсуляции контента в сложные изображения, когда проявляющиеся искажения могут быть практически незаметны; 2 - независимо от размера используемых субблоков (*смоделировано для случаев 8×8, 16×16, 32×32*), изображения-контейнеры со сложной структурой, с точки зрения стеганографических преобразований, всегда имеют неизменно больший потенциал (*лучшая способность к пространственному маскированию визуально фиксируемых артефактов, соответственно и низкая демаскировка факта выполненной стегановставки*).

Проведенные эксперименты подтвердили серьезное влияние значения порога загрубления на «заполнение» контейнера и качество восстановление самого контента (характерный пример представлен на рис. 9).



а) Pz = 20

б) Pz = 1

Рис. 9 – Восстановленный контент с «простой» структурой *(типа мнемосхема)* для разных значений P_Z

Так, при увеличении P_Z результирующий коэффициент сжатия будет большим (*т.к. формируется меньшее количество ОБ*) и уменьшается общее время кодирования (*время обработки стеганоконтента*), и наоборот, при уменьшении значения P_Z формируется больше ОБ и увеличивается время обработки. Однако, увеличение значения P_Z влияет на качество восстановления инкапсулированных изображений в худшую сторону (динамика процесса хорошо видна на рис.9), т.к. наблюдается результат работы блока ускорителя (*формирование подобных блоков*). И напротив, при уменьшении P_Z возрастает количество ОБ, что позитивно скажется на характеристиках визуализации изображения-контента, однако при этом увеличится количество артефактов в изображении-контейнере.

Другими словами, в процессе определения требуемого значения P_Z необходимо соблюдение баланса между качеством (*степенью сжатия*) визуализации скрываемого контента и интенсивностью, и характером визуализации артефактов, демаскирующих процесс выполненной стегановставки в изображение – контейнер.

Как следует из результатов моделирования, существенным фактором, влияющим на природу и интенсивность фиксируемых искажений изображений-контента, является характер использования/расстановки ОБ. Так, даже при обработке изображений с относительно простой структурой могут возникнуть довольно заметные искажения при его восстановлении (*дорожки повторяющихся блоков* на рис. 9). Ошибки вызваны тем, что сравниваются только max и min значения элементов в соседних блоках (*безотносительно позиции их размещения*). Поэтому при сравнении содержания соседних блоков, фактические значения могут не выходить за указанные пределы P_Z , и как следствие, алгоритмом формируются целые серии верных по содержанию, но ошибочных по структуре ОБ.

Упрощенный пример такой ситуации представлен на рис.10. В данном случае имеем фрагмент изображения (рис.4а), содержащий последовательность из 4-х блоков с одинаковыми значения яркости пикселов, но их различным размещением в каждом из блоков.

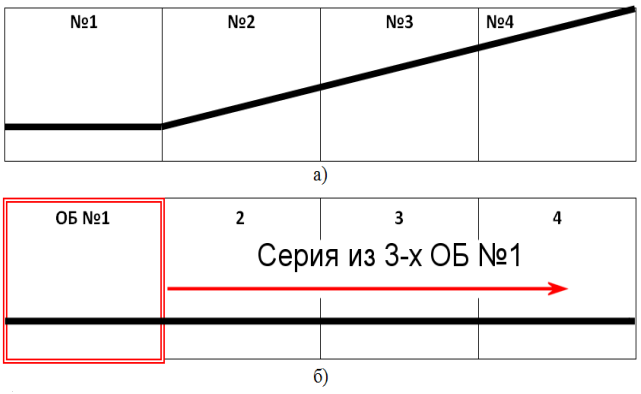


Рис. 10 – Результат формирования ОБ
(по старой схеме)

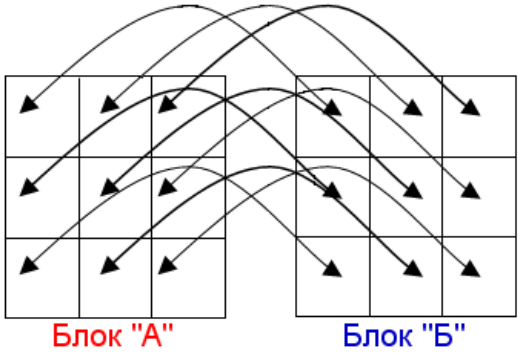


Рис. 11 – Поэлементное сравнение
(усовершенствованная схема)

Так в 1-м блоке есть горизонтальная линия, которая в начале 2-го блока меняет свое направление (поднимается). В результате работы алгоритма по «старой» схеме (рис. 1), при формировании серий ОБ, разница max и min значений перепада яркости элементов в соседних блоках будет неизменной и находиться в границах заданного значения P_Z. Поэтому при формировании серии ОБ, «родные» значения элементов в блоках №№ 2,3,4, естественно, не сохраняются (рис.10 б). Последствия такой обработки видны на рис. 9.

Для устранения указанного недостатка, используемый механизм был несколько доработан (рис.11). В его усовершенствованной версии производится позиционное сравнение элементов в соседних блоках.

Пример результата применения «старой» и доработанной схемы обработки представлен на рис.12 (*для контента с простой структурой (типа мнемосхема)*).

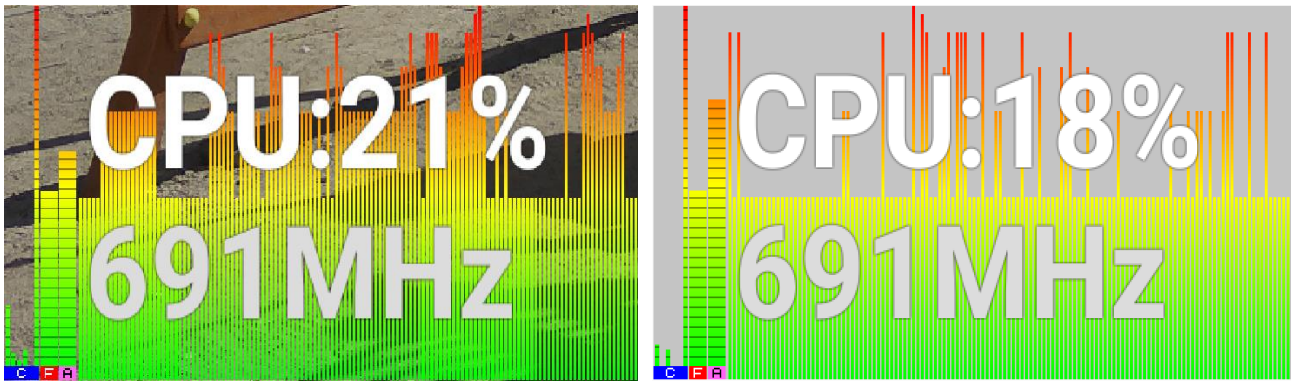
Из приведенного примера следует, что указанная доработка позволила ощутимо улучшить параметры восстановления скрываемого контента при относительно небольшом изменении количества ОБ (*мене чем на четверть*).

Тестовые испытания алгоритма проводилось на смартфоне под управлением ОС Android v. 6.0.1 Marshmallow® (*для данной версии ОС Android® актуальна версия Android SDK API v23*). Адаптация программного кода алгоритма велась с использованием среды разработки Intellij IDEA 2017.1.1.

а) n=8; P_Z =3; ОБ 1435; *б) n=8; P_Z =3; ОБ 1708*

Рис. 12 – Результаты восстановления контента для старой (а) и новой (б) схем формирования ОБ

Исследования тестовой версии алгоритма проводились с параметрами разрешения экрана смартфона 1080×1920 и частотой обновления 60Hz.



а) *б)*

Рис. 13 – Результаты измерений до запуска алгоритма (а) и в ходе его работы (б), где:
C – загрузка процессора; F – частота процессора; A – потребление АБ.
Прим.- указатели индикаторов размещаются в левой нижней части экрана.

Рис. 14 – Пользовательский интерфейс приложения (*тест-версия*)

Для проведения измерений использовались специализированные мобильные приложения (*например, «Advanced Task Manager», «Cool Tool», «OS Monitor» и др.*), с помощью которых фиксировались соответствующие данные: - объем занятой оперативной памяти, состояние АБ, загрузка процессора и его тактовая частота. Оценка объемов занятой оперативной памяти выполнялась для субблоков различных размеров, при разных уровнях заряда бортовой АБ и в отсутствии выполнения сторонних приложений (*за исключением системных процессов*). Характерные показания измерений при работе запущенного тестового алгоритма представлены на рис. 13 *(для варианта с размером субблоков изображений 8×8 эл.)*.

На рис. 14 представлен вариант исполнения основной панели управления приложения. Графический интерфейс программной оболочки, реализующей тестовую версию алгоритма, имеет несколько функциональных разделов, обеспечивающих возможность независимого управления основными процедурами алгоритма (*рабочие папки, режимы выбора масок обфускации, размеры блоков, порог сглаживания, параметры симметрии алгоритма и др.*).

В результате проведения цикла экспериментов, удалось установить, что при использовании адаптивного варианта работы алгоритма (*без вмешательства человека в порядок формирования настроечных параметров алгоритма*), увеличивается общее время использования ресурса АБ мобильного устройства (*особенно в режиме пакетной обработки данных*). Т.е. таким образом удалось подтвердить правильность выбранной концепции создания алгоритма: - согласование основных параметров работы алгоритма с текущими характеристиками и условиями работы мобильной платформы.

На рис. 15 представлены типовые значения загрузки процессора мобильного устройства (*обычно в диапазоне 12÷18 %*), характерные для случая выполнения полного цикла стеганографической обработки изображений (*без промежуточных стопов и формирования служебных данных телеметрии*).

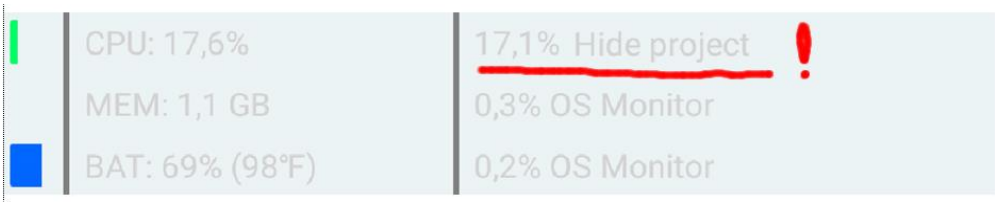


Рис. 15 – Результат измерения загрузки процессора при выполнении алгоритма

4 Выводы

1. Рассмотренный алгоритм обеспечивает режим адаптивной малоресурсной инкапсуляции стеганоконтента различного типа в изображения – контейнеры соизмеримых размеров (*количество блоков контейнера всегда больше количества формируемых блоков контента*).

2. При встраивании и декодировании (*извлечении*) контента, ключевой информацией являются следующие параметры: - использованный размер субблоков; - параметр симметрии стегановставки; - идентификаторы масок внутриблочной и межблочной обфускации.

3. Предложенный алгоритм обеспечивает адаптацию параметров своей работы к типу и количеству (*пакетная обработка*) обрабатываемых данных с учетом текущих характеристик функционирования мобильной платформы. Этим обеспечивается согласование параметров работы алгоритма с текущей загрузкой и ресурсными возможностями устройства.

4. Представленный порядок обработки трансформант характеризуется простотой реализации, малой вычислительной сложностью и обеспечивает хорошие условия для последующей инкапсуляции стеганоконтента с использованием симметричной схемы стегановставки.

5. Для повышения скрытности и стойкости к несанкционированной экстракции стеганоконтента использован гибридный механизм обфускации, реализующий механизмы внутриблочного и межблочного (внутрикадрового) перемешивания.

6. Сделан вывод о необходимости автоматизации процедуры выбора типа контейнера, в зависимости от характеристик инкапсулируемых данных.

7. Совершенствование рассмотренного алгоритма видится по следующим основным направлениям: – разработка эффективного механизма формирования масок межблочной обфускации; – развитие направления несимметричной обработки контейнера и контента; – комбинирование различных видов преобразований, в зависимости от типа обрабатываемого контента; – разработка механизма защиты от размножения ошибок стегановставки; – оптимизация параметров работы модуля «ускорителя» в зависимости от типа изображения – стеганоконтента; – формирование алгоритма скрытой трансляции видеоряда.

Ссылки

1. Gribunin, V.G. Tsifrovaya steganografiya / Gribunin V. G., Okov I. N., Turintsev I. V. – M.: Solon-Press, 2002. – 272 p.
2. Konakhovich, G.F. Komp'yuternaya steganografiya. Teoriya i praktika / Konakhovich G. F., Puzyrenko A.Yu. – K.: MK-Press, 2006. – 288 p.
3. Bykov, S.F. Algoritm szhatiya JPEG s pozitsii komp'yuternoi steganografii / Bykov S. F. // Zashchita informatsii. Konfident. – SPb.: 2000, № 3. pp. 26.
4. Prett, U. Tsifrovaya obrabotka izobrazhenii / U. Prett. – M.: Mir, 1985. – 736 p.
5. Zubarev, Yu. B. Tsifrovaya obrabotka televizionnykh i komp'yuternykh izobrazhenii / Yu.B. Zubarev, V.P. Dvorkovich. – Moskva: MTsNTI, 1997. – 212 p.
6. Korolev, A.V. Otsenka informativnosti transformant diskretnogo kosinusnogo preobrazovaniya / A.V. Korolev // Sistemi obrobki informatsiї. – 2003. – Vip.3. pp.81–85.
7. Malakhov, S.V., Bukhantsov, A.D. Zonal'noe kodirovanie izobrazhenii s razlichnym razbieniem prostranstvenno-chastotnoi oblasti / S.V. Malakhov, A.D. Bukhantsov // Sistemi obrobki informatsiї. – 2001. – Vip. 4(14). pp. 121–125.
8. Mastryukov, D. Algoritmy szhatiya informatsii. Ch.1. Szhatie po Khaffmenu // Monitor. - 1993. - № 7-8. pp.14-20.
9. Mastryukov, D. Algoritmy szhatiya informatsii. Ch.7. Szhatie graficheskoi informatsii // Monitor. - 1994. - № 6. pp.12-20.

Reviewer: Georgiy Kuchuk, Doctor of Technical Sciences, Full Professor, Professor of the Department of Computer Science and Programming, National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine.
E-mail: kuchuk56@ukr.net

Received: March 2018.

Authors:
Dmitriy Morozov, student of CSD, V. N. Karazin Kharkiv National University, Kharkov, Ukraine. E-mail: ikurortnik@gmail.com
Mykhailo Shaforostov, student of CSD, V. N. Karazin Kharkiv National University, Kharkiv, Ukraine.
E-mail: m61shaforostov@gmail.com
Serghii Malakhov, Ph.D., Senior Researcher, V. N. Karazin Kharkiv National University, Kharkiv, Ukraine.
E-mail: mailgate@meta.ua
Vadim Serbin, Leading Specialist, Yuzhnoye State Design Office, Dnipro, Ukraine. E-mail: buba75@i.ua

The double obfuscation of transformants of low-resource steganography algorithm.

Abstract. The purpose of the article is to familiarize with the basic procedures of the adaptive low-resource algorithm of steganography processing of images and the peculiarities of creation of its experimental program with support of the graphic interface (mobile application). The version of the program offered in operation provides convenience of its use on mobile platforms under control of the Android® operating system (OS). The adaptive algorithm in the manual and automatic modes is developed allows to define: - a current status of the hardware (a mobile platform); - take into account the features of processed data (types of images to a steganocontainer and to a steganocontent); - to adjust parameters of operation of main software modules of a research steganoalgorithm (the modul of preprocessing of input data (images), and the module of special conversions - the steganographic module). In addition, other parameters were investigated of image processing having direct influence on computing complexity of all algorithm and quality of visualization images of containers and steganocontent. Presented version of the algorithm is the research version and is an instrument for ensuring of the security of personal information (in this case the graphic information) users, first of all, of mobile gadgets. The main properties of the synthesized algorithm, allow classifying it as software of steganography protection, localized for conditions intraframe processed of images. Presented version of the algorithm requires its subsequent enhancement and has the main goal to confirm correctness of the selected methods of data handling and strategies of creation of the user interface for corresponding mobile application.

Keywords: obfuscation; encoding with conversion; zonal encoding; steganography.

Рецензент: Георгій Кучук, д.т.н., проф., НТУ «ХПІ», м. Харків, Україна.
E-mail: kuchuk56@ukr.net

Надійшло: Березень 2018.

Автори:
Дмитро Морозов, студент ФКН, ХНУ імені В. Н. Каразіна, м. Харків, Україна. E-mail: ikurortnik@gmail.com
Михайло Шафоростов, студент ФКН, ХНУ імені В. Н. Каразіна, м. Харків, Україна. E-mail: m61shaforostov@gmail.com
Сергій Малахов, к.т.н., с.н.с., ХНУ імені В. Н. Каразіна, м. Харків, Україна. E-mail: mailgate@meta.ua
Вадим Сербін, провідний фахівець, ДП «Конструкторське бюро «Південне», м. Дніпро, Україна. E-mail: buba75@i.ua

Подвійна обфускація трансформант малоресурсного стеганоалгоритма.

Анотація. Метою статті є ознайомлення з основними процедурами адаптивного малоресурсного алгоритму стеганографічної обробки зображень і особливостями створення його експериментальної програми з підтримкою графічного інтерфейсу (мобільного додатка). Запропонована версія програми орієнтована на зручність її використання на мобільних платформах під управлінням операційної системи (ОС) Android®. Розроблений адаптивний алгоритм в ручному та автоматичному режимах, дозволяє: - визначати поточний статус апаратного забезпечення (мобільної платформи); - враховувати особливості оброблюваних даних (типи зображень стеганоконтейнера і стеганоконтента); - коригувати параметри роботи основних програмних модулів дослідного стеганоалгорітма (блоку первинної обробки вхідних даних (зображень) і блоку спеціальних перетворень - стеганомодулю). Крім того, проаналізовано і інші параметри обробки зображень, що мають безпосередній вплив на обчислювальну складність всього алгоритму та якість візуалізації зображень контейнерів і стеганоконтента. Розглянута версія алгоритму є дослідною та служить засобом забезпечення безпеки персональних даних (в даному випадку графічної інформації) користувачів, перш за все, мобільних гаджетів. Основні властивості синтезованого алгоритму дозволяють класифікувати його, як програмний засіб забезпечення стеганографічної захисту, що локалізоване для умов внутрішньокадрової обробки зображень. Представлена версія алгоритму вимагає його подальшого вдосконалення і має своєю головною метою підтвердити правильність обраних методів обробки даних та стратегії створення користувальницького інтерфейсу відповідного мобільного додатку.

Ключові слова: обфускація; кодування з перетворенням; зональне кодування; стеганографія.