Учреждение образования
«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ»

УДК 004.056

СЕЙЕДИ
Сейедамин Мирхоссейн

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ СТЕГАНОГРАФИЧЕСКИХ АЛГОРИТМОВ НА ОСНОВЕ ВЕЙВЛЕТ-ПРЕОБРАЗОВАНИЙ

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

по специальности 05.13.19 – Методы и системы защиты информации,
информационная безопасность

Минск 2014

Научная работа выполнена в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники».

Научный руководитель **Иванов Николай Николаевич**, кандидат физико-математических наук, доцент, доцент кафедры электронных вычислительных машин учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»

Официальные оппоненты: **Дудкин Александр Арсентьевич**, доктор технических наук, доцент, главный научный сотрудник лаборатории № 222 идентификации систем ГНУ «Объединенный институт проблем информатики Национальной академии наук Беларуси»

Борискевич Анатолий Антонович, кандидат технических наук, доцент, доцент кафедры сетей и устройств телекоммуникаций учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»

Оппонирующая организация: **Белорусский государственный университет**

Защита состоится «13 ноября» 2014 г. в 14.00 на заседании совета по защите диссертаций при учреждении образования «Белорусский государственный университет информатики и радиоэлектроники» по адресу: 220013, г. Минск, ул. П. Бровки, 6, корп. 1, ауд. 232, тел. 293-89-89, e-mail: dissovet@bsuir.by.

С диссертацией можно ознакомиться в библиотеке учреждения образования «Белорусский государственный университет информатики и радиоэлектроники».

Автореферат разослан « 10 » октября 2014 г.

КРАТКОЕ ВВЕДЕНИЕ

В настоящее время системы связи и Интернет играют важную роль в передаче и обмене данными. При возрастании объемов обмена данными возрастает необходимость в предотвращении несанкционированного доступа к ним. Это приводит к новым тенденциям в передаче конфиденциальных данных, среди которых можно особо отметить стеганографию. Стеганография – это наука и техника сокрытия конфиденциальных данных в медиа-файл путем сохранения в тайне самого факта передачи, таким образом, что никто, кроме отправителя и получателя, не знает о наличии секретного сообщения. Стеганография способствует развитию стеганоанализа – методов выявления скрытого сообщения в передаваемом файле. Стеганография и стеганоанализ – два параллельно развивающихся направления науки. В стеганографии наиболее актуальным вопросом является разработка новых методов, преобладающих над методами стеганоанализа.

Цифровая стеганография основана на сокрытии данных в цифровых файлах-контейнерах, вызывая при этом искажения контейнера. Контейнером могут быть цифровые изображения, видео-, аудиофайлы, текст и т.п. Внесение искажений, которые находятся ниже порога чувствительности органов чувств среднестатистического человека, не приводит к заметным их изменениям. В цифровой стеганографии основные методы встраивания секретных сообщений разделяются на два класса – пространственные и – частотные. Методы частотной области вычислительно сложны и позволяют встраивать сообщения меньшей емкости по сравнению с пространственными методами. Но они являются более стойкими к методам стеганоанализа.

Свободный выбор контейнера является особым преимуществом методов стеганографии по сравнению с другими методами сокрытия информации. Обоснованный выбор подходящего изображения-контейнера может существенным образом повлиять на результат, потому что встраивание сообщения в разные контейнеры может дать существенно различные результаты, полученные при использовании конкретного метода. До сих пор эта задача упоминалась только в нескольких публикациях. Обычно алгоритмы с приоритетом по стойкости к атакам взломщика стеганосистемы не позволяют встроить в изображение секретную информацию значительного объема. Практика требует алгоритмов встраивания, которые, с одной стороны, повышают объем сообщения, а с другой стороны, лишь незначительно ухудшают качество контейнера. Наряду с методикой выбора подходящего контейнера и методов встраивания с приоритем по стойкости, в настоящее время одной из актуальных задач является задачи разработки новых алгоритмов обеспечения требуемого компромисса между объемом секретного сообщения и

качеством стего-изображения. данных, которые выдерживают разумный баланс между двумя указанными параметрами.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Связь работы с крупными научными программами

Исследования проводились на кафедре электронных вычислительных машин учреждения образования «Белорусский государственный университет информатики и радиоэлектроники» в рамках научно-исследовательской госбюджетной темы ГБ № 11-2019 «Методы и алгоритмы параллельной обработки изображений и видеопоследовательностей, распознавания объектов в режиме реального времени».

Цель и задачи исследования

Целью диссертационной работы является разработка стеганографических алгоритмов с использованием вейвлет-преобразований, обеспечивающих требуемое соотношение стеганографической емкости и стойкости на основе выбора подходящего контейнера.

Для достижения поставленной цели необходимо решить следующие задачи:

1. Изучить методы стеганографической защиты информации, методы стеганоанализа и методы атак на стеганосистемы.
2. Исследовать зависимость эффективности алгоритмов встраивания скрытых сообщений от вида контейнеров и секретных сообщений.
3. Разработать алгоритм сокрытия данных для обеспечения высокого уровня стойкости стеганосистемы, а также к атакам на обнаружение факта стеганографического сокрытия данных за счет выбора контейнера.
4. Разработать алгоритм встраивания сообщения для обеспечения передачи максимально возможного объема данных при численно заданных параметрах стеганосистемы, характеризующих степень искажения контейнера.
5. Разработать алгоритм сокрытия данных, обеспечивающий компромисс между объемом секретного сообщения и качеством стего-изображения.

Научная новизна

Разработана методика классификации изображений для выбора надлежащего контейнера на основе анализа разброса интенсивностей пикселей

изображения и энтропии изображения. Классификация позволяет разделить изображения на классы по их соответствию требованиям пользователя.

Предложены принципы построения стеганографических систем, оптимизированные по выбранным пользователем критериям, включая критерий стойкости к атакам на стего-изображение, критерий максимального объема встраиваемого сообщения при сохранении незаметности стеганосистемы и получения требуемого соотношения между объемом встраиваемого сообщения и незаметности сообщения в стего-изображении.

Объектом исследования являются стеганографические системы сокрытия данных с помощью вейвлет-преобразований.

Предметом исследования являются методы и алгоритмы повышения незаметности, емкости и стойкости стеганографических систем.

Положения, выносимые на защиту

1. Методика двухуровневой классификации изображений, направленная на выбор наиболее подходящего контейнера на основе анализа отклонения от среднего и вычисления энтропии каждого блока изображения, что позволяет разделить контейнеры на классы и оценить степень их пригодности для обеспечения стеганографических требований.

2. Алгоритм сокрытия данных с приоритетом по стойкости к атакам на обнаружение факта сокрытия данных путем разбиения контейнера на блоки и применения к блокам трехуровневого лифтингового вейвлет-преобразования, модифицируемые коэффициенты выбираются методом нуль-дерева.

3. Алгоритм сокрытия данных с приоритетом по объему встраиваемого сообщения при обеспечении требуемого уровня незаметности, основанный на разбиении контейнера на блоки, к которым применяется двухуровневое целочисленное вейвлет-преобразование Хаара, сообщение внедряется в коэффициенты блока в зависимости от их значений.

4. Адаптивный алгоритм сокрытия данных, обеспечивающий требуемое соотношение между объемом скрываемого сообщения и качеством стего-изображения, в основе алгоритма лежит двумерное целочисленное лифтинговое вейвлет-преобразование, модифицируются коэффициенты среднечастотной подматрицы в зависимости от величины их отклонения от среднего значения блока и энтропии блока.

Личный вклад соискателя

Постановка задач, математические модели и обсуждение результатов проводились с научным руководителем канд. физ-мат. наук Н.Н. Ивановым.

Алгоритмы разработаны соискателем самостоятельно. Соавторы опубликованных работ Р.Х. Садыхов и Н.Н. Иванов принимали участие в проведении экспериментальных исследований и обсуждении их результатов. Проектирование и разработка программного обеспечения выполнены автором самостоятельно.

Апробация результатов диссертации

Основные положения и результаты диссертационной работы докладывались и обсуждались на следующих конференциях: 49-я научная конференция аспирантов, магистрантов и студентов «Компьютерные системы и сети» (БГУИР, Минск, Беларусь, 2013 г.); Международная конференция «Information Technologies and Systems (ITS)» (БГУИР, Минск, Беларусь, 2013 г.); Международная научно-техническая конференция, приуроченная к 50-летию МРТИ–БГУИР (БГУИР, Минск, Беларусь, 2014 г.); XII Белорусско-российская научно-техническая конференция «Технические средства защиты информации» (БГУИР, Минск, Беларусь, 2014 г.).

Опубликованность результатов диссертации

По результатам исследований, представленных в диссертации, опубликовано 11 печатных работ, в том числе 7 статей в научных рецензируемых журналах, 4 статьи в материалах конференций общим объемом 4,65 авторских листов.

Структура и объем диссертации

Работа состоит из введения, четырех глав, заключения, библиографического списка и приложении. Общий объем диссертационной работы составляет 114 страниц, из них 71 страницы текста, 32 рисунка на 20 страницах, 15 таблиц на 5 страницах, 2 приложения на 5 страницах, библиография из 129 источников на 13 страницах, включая 11 публикаций автора на 2 страницах.

ОСНОВНАЯ ЧАСТЬ

В **первой главе** проведен обзор опубликованных работ, рассмотрены основные объекты стеганографической системы: контейнер (исходный и заполненный), встраиваемое сообщение, ключ, методы встраивания и извлечения и рассмотрены критерии оценок стеганографических систем. Проведен анализ известных методов встраивания данных в пространственной и частотной областях представления изображения [1] и методы стеганоанализа, а также исследована характеристика атак на стеганографические системы.

Проведенный в рамках первой главы анализ показывает, что:

– известны методы стеганографической модификации изображений, осуществляющие сокрытие сообщений с использованием как пространственной, так и частотной области представления контейнеров. Эти методы обладают как достоинствами, так и недостатками, которые необходимо учитывать при создании стеганографической системы [1, 2];

– статистические методы стеганоанализа являются более надежными и дают более точные результаты вследствие их большей чувствительности к незначительным модификациям контейнеров по сравнению с визуальными методами стеганоанализа [4];

– актуальной задачей является разработка алгоритмов на основании вейвлет-преобразований, обеспечивающих высокий уровень стойкости стеганосистемы к атакам; согласованный выбор контейнера и встраиваемого сообщения при обеспечении передачи максимально возможного объема данных с численно заданными параметрами стеганосистемы; обеспечивающих требуемый компромисс между объемом секретного сообщения и качеством стего-изображения.

Для повышения эффективности алгоритмов встраивания секретных сообщений во **второй главе** предложена классификация контейнеров-изображений. Для выбора наиболее подходящего стеганографического контейнера при заданных требованиях к стеганографической системе в работе предложена методика двухуровневой статистической классификации контейнеров-изображений [9]. На первом уровне осуществляется разделение всех изображений, разбитых на непересекающиеся блоки размером 3×3 пикселя, на четыре класса по количеству входящих в него блоков, отнесенных к негладкому типу. Этот тип блока характеризуется превышением максимального отклонения интенсивностей элементов блока от среднего значения интенсивности по всем блокам изображения [3]. Схема алгоритма первого уровня классификации представлена на рисунке 1. На втором уровне классификации осуществляется ранжирование изображений в пределах полученных классов по степени их текстурной неоднородности, оцениваемой

по энтропии блоков размером 8×8 [3]. Схема алгоритма второго уровня классификации представлена на рисунке 2.

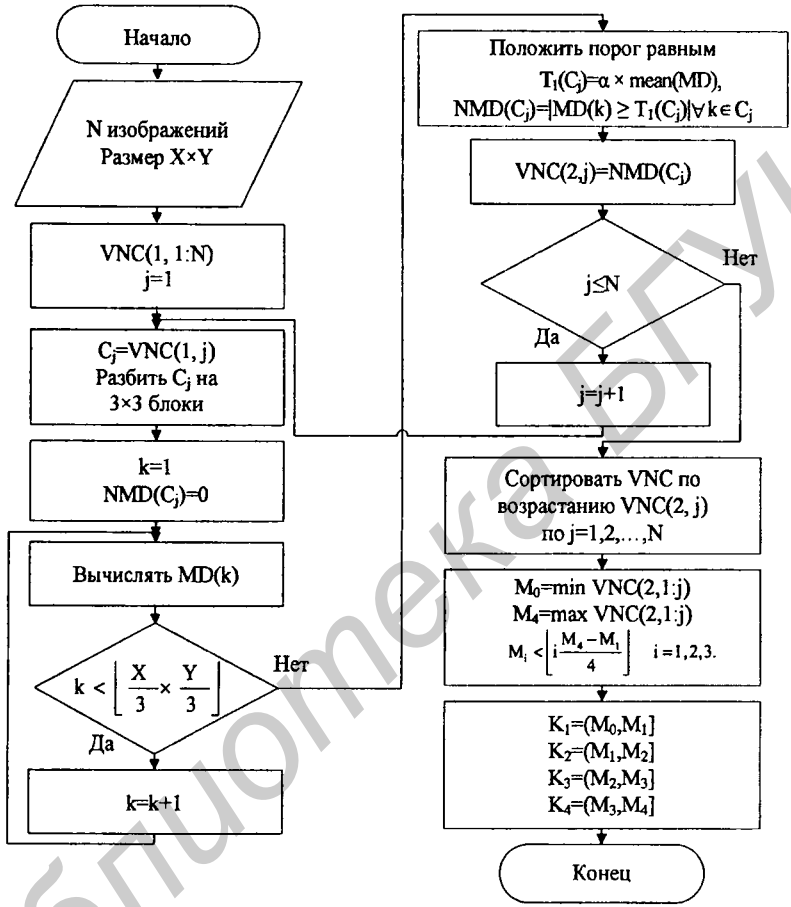

Рисунок 1. – Схема алгоритма первого уровня классификации

Для стеганографических систем характерно снижение стойкости стеганосистемы с увеличением объемов встраиваемых данных [10]. **Третья глава** посвящена построению алгоритмов встраивания с оптимизацией по выделенным критериям. В работе предложены три алгоритма: 1) алгоритм с приоритетом по стойкости к атакам на обнаружение факта сокрытия данных; 2) алгоритм с приоритетом по встраиванию наибольшего объема данных при обеспечении численно заданных параметров стеганосистемы; 3) адаптивный алгоритм, обеспечивающий требуемое соотношение объема скрываемого сообщения к критерию незаметности стеганосистемы [4–7].

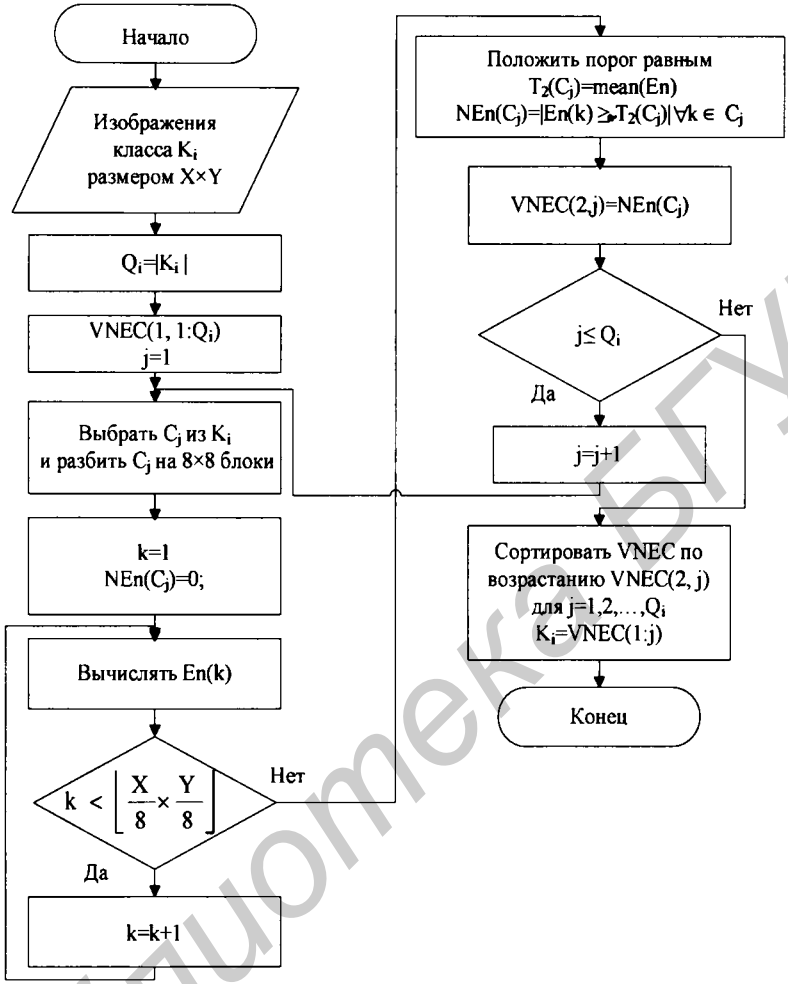

Рисунок 2. – Схема алгоритма второго уровня классификации

Алгоритм с приоритетом по стойкости построен на основании разделения контейнера на непересекающиеся блоки размером 8×8 пикселей, к каждому из которых применяется трехуровневое лифтинговое вейвлет-преобразование. Коэффициенты преобразования разделяются на значимые и незначимые с использованием метода нуль-дерева. Среди незначимых коэффициентов выделяют корневые коэффициенты, в которые методом замены наименее значащих бит встраиваются фрагменты секретного сообщения [5]. Схема алгоритма встраивания скрытия данных представлена на рисунке 3.

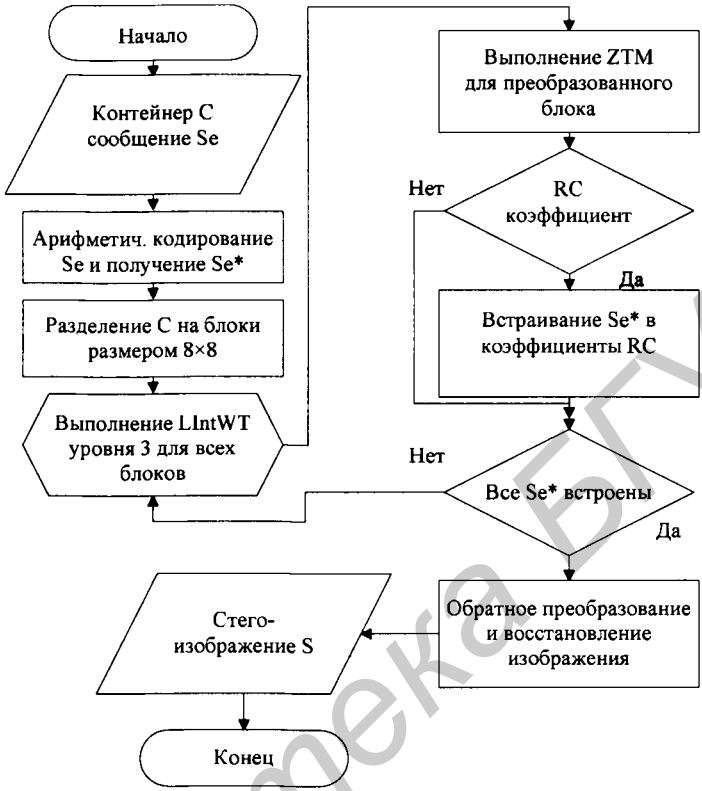

Рисунок 3. – Схема алгоритма встраивания с приоритетом по стойкости

Алгоритм сокрытия данных с приоритетом по объему встраиваемого сообщения также использует разделение контейнера на блоки [11]. Вначале выравнивается гистограмма контейнера, после чего он разделяется на непересекающиеся блоки, к которым применяется двухуровневое целочисленное вейвлет-преобразование Хаара. Коэффициенты преобразованного блока k по их абсолютным величинам делятся на незначимое E и значимое U подмножества. Коэффициент блока k принадлежит подмножеству E, если его абсолютное значение меньше половины абсолютного максимального значения вейвлет коэффициента блока k. Сообщение встраивается в коэффициенты множества E в соответствии с выбранным порогом. Количество встраиваемых бит секретного сообщения в коэффициенты подмножества E в блоке k определяется абсолютным значением этих коэффициентов [6]. Схема алгоритма с приоритетом по объемам встраиваемых сообщений представлена на рисунке 4.

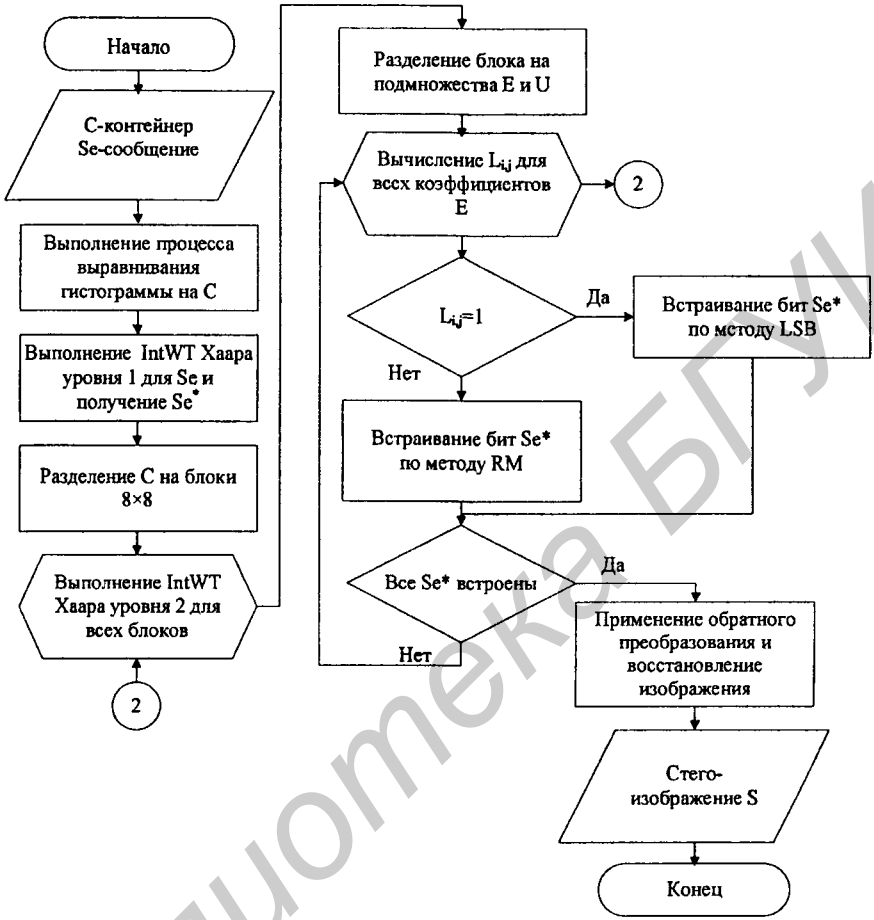

Рисунок 4. – Схема алгоритма с приоритетом по объему встраивания

Адаптивный алгоритм, обеспечивающий требуемое соотношение между объемом скрываемого сообщения и качеством стего-изображения, начинает работу также с выравнивания гистограммы контейнера. После этого применяется целочисленное лифтинговое вейвлет-преобразование. Коэффициенты его среднечастотной подматрицы разделяются на непересекающиеся блоки размерностью 4×4. Полученные блоки по величине отклонения от среднего значения элементов блока и величине их энтропии разделяются на три класса: гладкие, сильно неоднородные и текстурные блоки. Гладкие блоки не модифицируются, в коэффициенты сильно неоднородных

блоков встраиваются по три, а в текстурные блоки по два бита секретного сообщения [7]. Схема алгоритма представлена на рисунке 5.

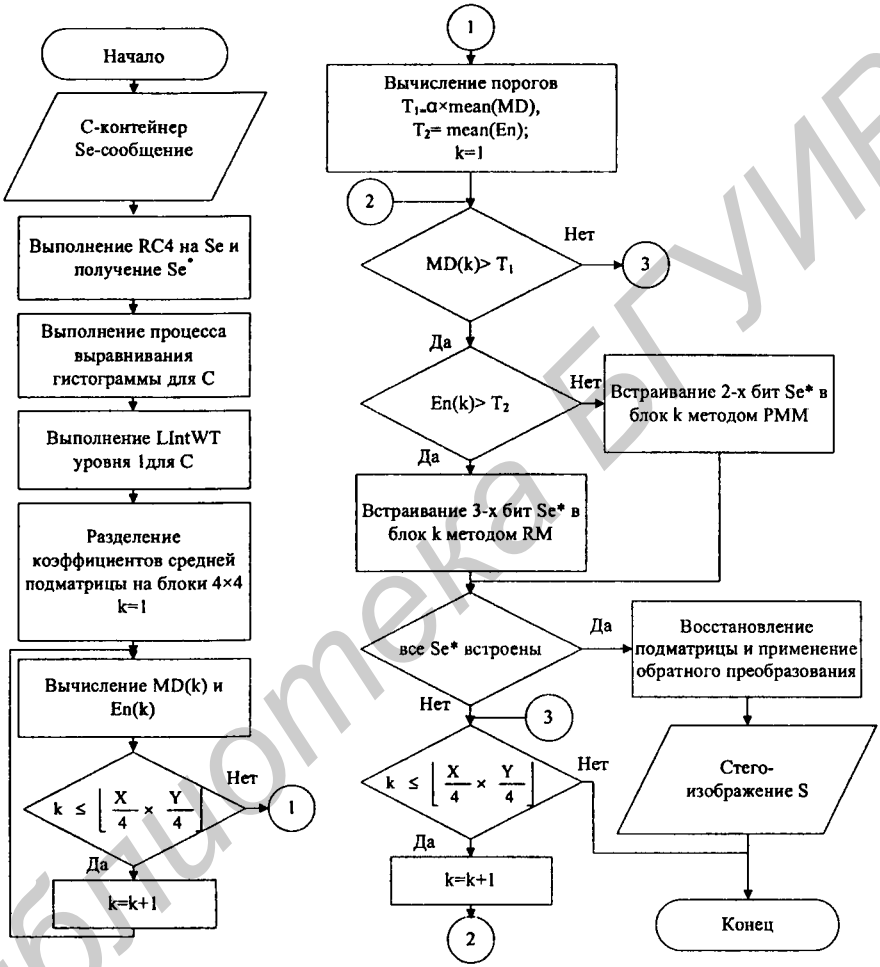

Рисунок 5. – Схема адаптивного алгоритма встраивания с соотношением объем/качество

В **четвертой главе** исследованы оценки эффективности предложенных алгоритмов по общепринятым критериям емкости, незаметности и стойкости. Емкость измеряется размером встраиваемого сообщения. Для незаметности есть несколько критериев, например MSE, PSNR и др. Стойкость оценивается ε-стойкостью Кульбака-Лейблера и методами стеганоанализа.

Для эксперимента использовались 1000 контейнеров из известных баз изображений. Секретное сообщение Se генерировалось случайным образом.

Результаты оценок алгоритма скрытия данных с приоритетом по стойкости на обнаружение факта сокрытия данных приведены в таблицах 1–2, где алгоритм сравнивается с известными алгоритмами S. Bhattacharyya и H. Reddy по критериям стеганографической емкости и незаметности. Стойкость предложенного алгоритма оценивалась мерой ε-стойкости (таблица 3) и универсальными статистическими показателями качества стего-изображения IQM. В главе показано, что статистическая разница между контейнерами и стего-изображенями при использовании предложенного алгоритма, обеспечивающего высокую стойкость стеганосистемы, меньше, чем у алгоритма H. Reddy [4, 5].

Таблица 1. – Сравнение емкости предложенного алгоритма, обеспечивающего высокую стойкость стеганосистемы, с алгоритмами S. Bhattacharyya и H. Reddy

Контейнер	Размер	Емкость Reddy (бит)	Емкость Bhattacharyya (бит)	Емкость предложенного алгоритма (бит)
«Лена»	128×128	2048	2240	5145
	256×256	8192	9536	20622
	512×512	32768	40048	82578
«Перец»	128×128	2048	2832	5223
	256×256	8192	11440	20694
	512×512	32768	46776	83846

Таблица 2. – Сравнение значения PSNR при встраивании в контейнер «Лена» сообщений различного объема

Размер контейнера	Объем сообщения (char)	PSNR CA(B)	PSNR CH(B)	PSNR CV(B)	PSNR CD(B)	PSNR алгоритма Reddy	PSNR предложенного алгоритма
128×128	100	53,29	54,91	54,66	58,83	41,16	61,50
	200	50,66	52,35	51,94	56,90	36,29	58,38
	400	47,89	49,34	48,97	54,49	35,95	55,56
	500	47,03	48,36	48,03	48,02	35,61	54,76
256×256	100	59,77	62,36	62,34	58,83	57,93	66,71
	200	56,73	58,74	58,75	56,90	50,38	64,07
	400	53,69	55,43	55,55	54,49	43,43	61,17
	800	50,77	52,62	52,31	51,84	38,83	58,16
	1600	47,67	49,49	49,16	49,04	N/A	55,31
	2000	46,77	48,56	51,09	48,12	N/A	54,39

Алгоритм скрытия данных с приоритетом по объемам встраивания при заданном уровне незаметности более эффективен, чем алгоритмы D. Wu и B. Lai [11]. Таблица 4 дает сравнение критериев незаметности и ε-стойкости для

объема секретного сообщения 30000 байт, а также сравнивает емкость предложенного алгоритма с емкостями алгоритмов D. Wu и B. Lai. Стойкость в предложенном алгоритме выше на 18,3 и 92,06 %, а емкость алгоритма превышает емкости алгоритмов D. Wu и B. Lai на 10,62 и 16,34 % соответственно [6].

Таблица 3. – Сравнение критериев незаметности и стойкости предложенного алгоритма и алгоритма H. Reddy [4]

Объем сообщения (байт)	Метрика	Предложенный алгоритм		Алгоритм Reddy	
		Mean	Std. Dev.	Mean	Std. Dev.
4096	PSNR	57,33	0,121	37,42	4,232
	MSE	0,4618	0,0128	18,3505	18,48
	ε-стойкость	6,14E-06	3,95E-06	1,97E-04	1,59E-04
2916	PSNR	58,72	0,485	39,35	4,1972
	MSE	0,0878	0,0097	11,8814	12,98
	ε-стойкость	4,47E-06	2,98E-06	3,36E-04	1,95E-04
1936	PSNR	60,49	0,551	41,96	4,223
	MSE	0,0585	0,0073	6,8104	9,225
	ε-стойкость	2,91E-06	2,01E-06	1,97E-04	1,6E-04

Таблица 4. – Сравнение критериев незаметности и стойкости стего-изображений

Метрика	Алгоритм Wu		Алгоритм Lai		Предложенный алгоритм	
	Mean	Std. Dev.	Mean	Std. Dev.	Mean	Std. Dev.
PSNR	41,13	1,492	40,25	1,268	42,06	1,338
MSE	6,247	4,790	5,758	1,492	4,2313	1,35
ε-стойкость	2,02E-04	1,2E-04	1,31E-03	3,4E-03	1,65E-04	8,81E-05
Емкость (бит)	422376	–	401615	–	467266	–

В главе показано, что статистическая разница между контейнерами и стего-изображениями предложенного алгоритма с приоритетом по объемам встраивания меньше, чем у упомянутых алгоритмов [6].

Для алгоритма, который обеспечивает требуемое соотношение объема сообщения к незаметности стеганосистемы, эксперименты были выполнены с модификацией среднечастотной подматрицы (HL) вейвлет-преобразования. Эксперименты показали, что емкость предложенного алгоритма имеет прямую связь с параметром α алгоритма. Рисунок 6 показывает величину емкости для разных значений α [7]. При уменьшении значения фактора α качество стего-изображения ухудшается, так как в этом случае выбранные области для

встраивания секретного сообщения в большей степени относятся к гладким областям.

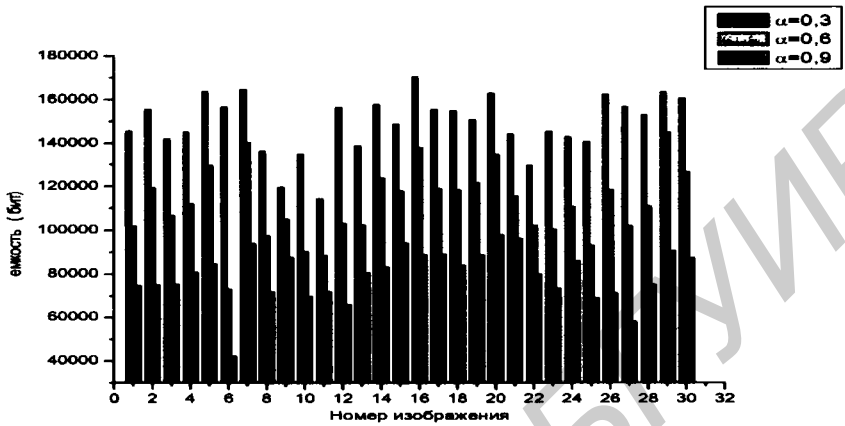

Рисунок 6. – Величина емкости контейнеров для различных значений α

Сравнение критериев рассматриваемого алгоритма с аналогичными параметрами алгоритма Y. Wang показано в таблице 5, объем сообщения равен 6000 байт, показаны средние значения для 1000 изображений. Предложенный алгоритм обладает лучшими показателями PSNR и MSE по сравнению с алгоритмом Y. Wang, превышение показателей на 3–6 % [7].

Таблица 5. – Сравнение критериев незаметности стего-изображений

Метрика	Предложенный (α=0,3)		Предложенный (α=0,6)		Предложенный (α=0,9)		Алгоритм Y. Wang	
	Mean	St. Dev	Mean	St. Dev	Mean	St. Dev	Mean	St. Dev
PSNR	42,53	1,30	43,98	2,10	45,25	2,65	42,57	0,74
MSE	3,78	1,08	2,79	1,21	2,12	1,02	3,65	0,59

Таким образом, в главе исследованы зависимости между объемами встраиваемых данных, стойкостью и незаметностью для трех предложенных алгоритмов. Эксперименты показали, что показатели емкости, ε-стойкости и незаметности у предложенных алгоритмов в основном лучше, чем у известных стеганосистем.

В **приложении** приведены экранные копии, описание пользовательского интерфейса разработанного комплекса «Stegano Framwork», акты об использовании результатов диссертационной работы.

ЗАКЛЮЧЕНИЕ

Основные научные результаты диссертации

В диссертационной работе разработаны новые частотные алгоритмы стеганографии. Методы сокрытия информации в частотной области более надежны по сравнению с методами встраивания в пространственной области [1, 2, 8]. В диссертацинной работе получены следующие результаты, обладающие научной новизной:

1. Методика двухуровневой классификации, на первом уровне которой изображения классифицируются на основе анализа их гладкости, на втором – полученные классы ранжируются по текстуре. Преимущество этой методики состоит в оценке пригодности использования изображения в качестве контейнера, сформулированы правила для выбора контейнера, удовлетворяющего заданным стеганографическим требованиям. Отличие от существующих методик выбора контейнеров для стеганографии, опубликованных в работах Z. Kermani, S. Sadkhan, Y. Sun, заключается в двух уровнях классификации, предложенной в диссертации, и в том, что предложенная классификация учитывает все три основных типа критериев качества стего-изображения [3, 9].

2. Алгоритм сокрытия данных с приоритетом по стойкости к атакам пассивного взломщика. Контейнер разделяется на блоки, сообщение встраивается в коэффициенты блоков целочисленного вейвлет-преобразования с лифтингом. Модифицируемые коэффициенты выбираюся на основании метода нуль-дерева, модифицируются корневые коэффициенты дерева. По сравнению с широко распространными стеганографическими алгоритмами H. Reddy и S. Bhattacharyya, ε-стойкости увеличена в три раза, емкость на 50 %. Кроме того, по критериям IQMs предложенный алгоритм имеет большую стойкость к атакам пассивного взломщика, чем алгоритм H. Reddy [4, 5].

3. Алгоритм сокрытия секретного сообщения большого объема в контейнер при заданном уровне незаметности. Контейнер представляется в виде объединения однородных блоков. Коэффициенты двухуровневого целочисленного вейвлет-преобразования Хаара каждого блока разделяются на два подмножества. Секретное сообщение встраивается в коэффициенты вейвлет-преобразования в зависимости от абсолютного значения коэффициента. Алгоритм имеет емкость больше на 10,62 и 16,34 % чем алгоритмы D. Wu и B. Lai соответственно. Незаметность предложенного алгоритма больше на 2,26 и 4,49 % по сравнению с упомянутыми алгоритмами. Е-стойкость предложенного алгоритма выше на 18,3 и 92,06 %, чем у

упомянутых алгоритмов. Кроме того, критерии IQMs алгоритма лучше, чем у D. Wu и B. Lai [6, 11].

4. Адаптивный алгоритм сокрытия данных, обеспечивающий требуемое соотношение между объемом скрываемого сообщения и качеством стего-изображения. Контейнер преобразуется в частотную область целочисленным вейвлет-преобразованием с лифтингом. Модифицируются коэффициенты средних частот, которые выбираются по статистическим параметрам блоков, после чего проводятся изменения в сильно неоднородных и текстурных блоках. Алгоритм обладает незаметностью на 3–6 % большей, чем алгоритм Y. Wang с таким же объемом секретного сообщения [7].

5. Исследовано влияние типа секретного сообщения и вида операции, выполняемой над ним, в частотной стеганографии. Показано, что тип секретного сообщения не влияет на стойкость и незаметность. Сжатие с потерями позволяет уменьшить объем встраиваемых данных и уменьшает искажения контейнера [5,10].

6. Получены зависимости между объемами встраиваемых данных и стойкостью в предложенных алгоритмах. Эксперименты показали, что наилучшие показатели ε-стойкости достигаются у алгоритма, обеспечивающего высокую стойкость [5].

Рекомендации по практическому использованию результатов

1. В рамках выполнения темы ГБ № 11-2019 разработан специализированный программный стеганографический комплекс «Stegano Framework» для исследований методов стеганографии и исследования эффективности стеганографических алгоритмов.

2. Программный стеганографический комплекс «Stegano Framework» был протестирован на иностранном унитарном предприятии Годел Текнолоджис Юроп. Проверка показала, что стеганосистема успешно выполняет заявленные автором операции по внедрению и извлечению сообщений из изображений.

3. Разработанный программный стеганографический комплекс «Stegano Framework» внедрен в компаниях IH «Imen Hamrah» и BPJ «Behparzadeh Jahan» Республики Иран. Он используется для безопасного обмена конфиденциальной информацией, а также для защиты файлов базы данных от несанкционированного доступа.

4. Дальнейшие исследования будут нацелены на усовершенствование эффективности стеганографических алгоритмов встраивания в частотной области. В частности, это может быть выбор оптимальных базисных функций вейвлета. Кроме того, внимание следует уделить практическому применения полученных результатов.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ ПО ТЕМЕ ДИССЕРТАЦИИ

Статьи в научных журналах

1. Сейеди, С.А. Сравнение методов стеганографии в изображениях / С.А. Сейеди, Р.Х. Садыхов // Информатика. – 2013. – № 1(37). – С. 66–75.

2. Seyyedi, S.A. Digital Image Steganography Concept and Evaluation / S.A. Seyyedi, R.Kh. Sadykhov // International Journal of Computer Applications. – 2013. – Vol. 66, № 5. – P. 17–23.

3. Seyyedi, S.A. Statistical Image Classification for Image Steganographic Techniques / S.A. Seyyedi, N. Ivanov // International Journal of Image, Graphics and Signal Processing. – 2014. – Vol. 6, № 8. – P. 19–24.

4. Сейеди, С.А. Стек алгоритмов стеганографии изображений с применением вейвлетов и дерева нулей / С.А. Сейеди, Н.Н. Иванов // Электроника инфо. – 2013. – № 11. – С. 34–39.

5. Seyyedi, S.A. A Novel Secure Steganography Method Based on Zero Tree Method / S.A. Seyyedi, N. Ivanov // International Journal of Advanced Studies in Computer Science and Engineering. – 2014. – Vol. 3, № 3. – P. 1–9.

6. Seyyedi, S.A. High Payload and Secure Steganography Method Based on Block Partitioning and Integer Wavelet Transform / S.A. Seyyedi, N. Ivanov // International Journal of Security and Its Applications. – 2014. – Vol.8, № 4. – P. 183–194.

7. Seyyedi, S.A. An Adaptive Steganographic Method in Frequency Domain Based on Statistical Metrics of Image/ S.A. Seyyedi, N. Ivanov // International Journal of Cyber-Security and Digital Forensics. – 2014. – Vol. 3, № 1. – P. 63–71

Статьи в материалах научных конференций

8. Seyyedi, S.A. Secure Communication with Steganography Techniques / S.A. Seyyedi, N.N. Ivanov // Компьютерные системы и сети: материалы 49-й научной конференции аспирантов, магистрантов и студентов, Минск, 6–10 мая 2013 г. / БГУИР; под ред. В.А. Прыткова. – Минск, 2013. – С. 46–47.

9. Сейеди, С.А. Выбор изображения для стеганографического встраивания / С.А. Сейеди, Н.Н. Иванов // Технические средства защиты информации: материалы XII Белорусско-российской научно-технической конференции, Минск, 28–29 мая, 2014 г. / БГУИР, Минск, 2014. – С. 37.

10. Seyyedi, S.A. An Efficient Data Hiding Scheme Using Discrete Wavelet Transform / S.A. Seyyedi, N.N. Ivanov // Информационные технологии и

системы: материалы Междунар. науч. Конф., Минск, 23 октября 2013 г. / БГУИР; под ред. Л.Ю. Шилина. – Минск, 2013. – С. 318–319.

11. Seyyedi, S.A. An Adaptive Steganography Based on Partitioning Approach / S.A. Seyyedi, N.N. Ivanov // Материалы международной научно-технической конференции, приуроченной к 50-летию МРТИ–БГУИР, Минск, 18–19 марта 2014 г. Ч. 1 / БГУИР; под ред. А.А. Кураева. – Минск, 2014. – С. 374–375.

РЭЗЮМЭ

Сейедзі Сейедамін Мірхасейн

Павышэнне эфектыўнасці стэганаграфічных алгарытмаў на аснове вэйвлет пераўтварэнняў

Ключавыя словы: стэганаграфія, стэганааналіз, стэганасістэма, кантэйнер-малюнак, класіфікацыя малюнкаў, вэйвлет пераўтварэнні, метад нуль-дрэва.

Мэтай дысертацыйнай працы з'яўляецца распрацоўка алгарытмаў і методык лічбавай стэганографіі малюнкаў з павелічэннем аб'ёму схаванага паведамлення, павышэння стойкасці да нападаў узломшчыка, паляпшэння паказчыкаў незаўважнасці сакрэтнага паведамлення.

Метадамі даследавання з'яўляюцца вэйвлет пераўтварэнні. Сакрэтнае паведамленне ўкараняецца ў сярэднечастотныя каэфіцыенты пераўтварэння.

Атрыманы наступныя новыя вынікі.

Прапанавана методыка класіфікацыі малюнкаў на прадмет выкарыстання іх у якасці кантэйнераў, у якія ўкараняюцца сакрэтныя паведамленні. Выявы для падзелу на класы разбіваюцца на блокі, для кожнага блока вылічваецца ступень раскіданасці яго элементаў і энтрапія блока. У працы абгрунтоўваецца выбар класа ў адпаведнасці з запытамі карыстальніка.

Распрацаваны тры частотных стэганаграфічных алгарытмаў. Першы алгарытм выкарыстоўвае трохузроўневае цэлалікавае вэйвлет пераўтварэнне са схемай ліфтынгу. мадыфікаваныя каэфіцыенты вызначаюцца нуль-дрэвам. У другім алгарытме ўжываецца вэйвлет Хаара. Каэфіцыенты мадыфікуюцца ў залежнасці ад іх велічынь. У трэцім алгарытме зыходны малюнак пераўтвараецца біартаганальным вэйвлетам Коэна-Добеши-Фово са схемай ліфтынгу. Каэфіцыенты, у якія ўбудоўваецца паведамленне, мадыфікуюцца ў залежнасці ад значэння адаптыўіага парога. Эксперыменты паказалі перавагу прапанаваных алгарытмаў па параўнанні з агульнапрынятымі на крытэрыях ёмістасці, стойкасці і незаўважнасці.

Прапанаваныя алгарытмы можна выкарыстоўваць для бяспечнай перадачы канфідэнцыйнай інфармацыі па адкрытых камунікацыйных каналах, а таксама для бяспечнага захоўвання дадзеных.

Вобласцямі прымянення вынікаў могуць быць любыя арганізацыі, у якіх патрабуецца бяспечны абмен і захоўванне даных. Гэта камерцыйныя прадпрыемствы, адміністрацыйныя ўстановы, прадпрыемствы з інавацыйнымі тэхналогіямі, гандлёвыя пляцоўкі.

РЕЗЮМЕ

Сейеди Сейедамин Мирхоссейн

Повышение эффективности стеганографических алгоритмов на основе вейвлет-преобразований

Ключевые слова: стеганография, стеганоанализ, стеганосистема, контейнер-изображение, классификация изображений, вейвлет-преобразования, метод нуль-дерева.

Целью диссертационной работы является разработка алгоритмов и методик цифровой стеганографии изображений с увеличением объема скрытого сообщения, повышения стойкости к атакам взломщика, улучшения показателей незаметности наличия секретного сообщения в стеганографическом изображении.

Методами исследования являются вейвлет-преобразования. Секретное сообщение внедряется в среднечастотные коэффициенты преобразования.

Получены следующие новые результаты.

Предложена методика классификации изображений на предмет использования их в качестве контейнеров, в которые внедряются секретные сообщения. Изображения для разделения на классы разбиваются на блоки, для каждого блока вычисляется степень разбросанности его элементов и энтропия блока. В работе обосновывается выбор класса, из которого в соответствии с запросами отправителя выбирается контейнер.

Разработаны три частотных стеганографических алгоритма. Первый алгоритм использует трехуровневое целочисленное вейвлет-преобразование со схемой лифтинга. Модифицируемые коэффициенты определяются нуль-деревом. Во втором алгоритме применяется вейвлет Хаара. Коэффициенты модифицируются в зависимости от их величин. В третьем алгоритме исходное изображение преобразуется биортогональным вейвлетом Коэна–Добеши–Фово со схемой лифтинга. Коэффициенты, в которые встраивается сообщение, модифицируются в зависимости от значения адаптивного порога. Эксперименты показали преимущество предложенных алгоритмов по сравнению с общепринятыми по критериям емкости, стойкости и незаметности.

Предложенные алгоритмы можно использовать для безопасной передачи конфиденциальной информации по открытым коммуникационным каналам, а также для безопасного хранения данных.

Областями применения результатов могут быть любые организации, в которых требуется безопасный обмен и хранение данных. Это коммерческие предприятия, административные учреждения, предприятия с инновационными технологиями, торговые площадки.

SUMMARY

Seyyedi Seyyedamin Mirhossein

Improving the efficiency of steganographic algorithms based on wavelet transformation

Keywords: steganography, steganalysis, steganosystem, image container, classification of images, wavelet transform, zero tree method.

The aim of the thesis is the development of algorithms and techniques of digital image steganography to increase volume of the hidden message, and increase resistance to attack by a cracker, improvement in the invisibility of the existence of secret messages.

Research methods are wavelet transformation. The secret message is embedded in the middle frequency coefficients.

We obtained the following new results.

A method for classification of images for usage them as containers, which are embedded the secret messages. Image for division into classes is partitioned into blocks, the degree of dispersion of block's elements, and the entropy are evaluated for each block. The thesis substantiates the choice of the class in accordance with the needs of the user.

Furthermore, three steganographic algorithms in the frequency domain are proposed. The first algorithm uses a three-level integer wavelet transform with lifting scheme. Coefficients subject for modification are determined by the zero tree method. The second algorithm applies the Haar wavelet. The coefficients are modified depending on their magnitudes. In the third algorithm, the original image is converted by biorthogonal Cohen–Daubechies–Foveaux wavelet with the lifting scheme. Coefficients, into which a secret message is embedded, are modified depending on the value of the calculated threshold, multiplied by an adaptive factor. Experiments have shown the advantage of the proposed algorithms under capacity, security, and invisibility criteria in comparison with the conventional ones.

The proposed algorithm can be applied for secure transfer of confidential information via open communication channels, and for securely storing data.

Areas of application can be any organization that requires secure communication and data storage. Commercial enterprises, administrative institutions, enterprises with innovative technology, trading platforms are among them.

Научное издание

Сейеди Сейедамин Мирхоссейн

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ СТЕГАНОГРАФИЧЕСКИХ АЛГОРИТМОВ НА ОСНОВЕ ВЕЙВЛЕТ-ПРЕОБРАЗОВАНИЙ

Специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность

Автореферат диссертации на соискание ученой степени

Подписано в печать 06.10.2014.	Формат 60x84 $^{1}/_{16}$.	Бумага офсетная.
Гарнитура «Таймс».	Отпечатано на ризографе.	Усл. печ. л. 1,4.
Уч.-изд. л. 1,3.	Тираж 60 экз.	Заказ 390.

Издатель и полиграфическое исполнение: учреждение образования «Белорусский государственный университет информатики и радиоэлектроники».
Свидетельство о государственной регистрации издателя, изготовителя, распространителя печатных изданий №1/238 от 24.03.2014, №2/113 от 07.04.2014, №3/615 от 07.04.2014
ЛП №02330/264 от 14.04.2014.
220013, Минск, П. Бровки, 6