А.Г. Коробейников, С.С. Кувшинов, С.Ю. Блинов, А.В. Лейман

АНАЛИЗ ПРИНЦИПОВ СОЗДАНИЯ И РАБОТЫ СТЕГАНОГРАФИЧЕСКИХ АЛГОРИТМОВ

Аннотация: *Представлены основные задачи, решаемые при помощи стеганоалгоритмов в медиа-пространстве. Рассмотрены основные элементы стегосистемы. Проанализированы основные свойства и дана классификация для систем цифровых водяных знаков (ЦВЗ). Проведен анализ основных направлений разработки и функционирования современных стеганографических алгоритмов. Проанализированы стеганоалгоритмы для графических контейнеров.*

Ключевые слова: *Программное обеспечение, графический контейнер, классификация стегосистем ЦВЗ, медиапространство, стегасистема, стеганоалгоритмы пространственной области, стеганоалгоритмы области преобразования, форматные методы, ЦВЗ, цифровые изображения*

Введение

В настоящее время использование цифровых форматов мультимедиа становится повсеместным [1]. Но наряду с этим в современном информационном обществе, исследования и разработки в области стеганографии становятся все более популярными. Это связано с тем, что существуют проблемы управления цифровыми ресурсами и контроля использования прав собственности на компьютерные файлы. Отсюда возникает актуальнейшая задача сокрытия информации в условиях развитой инфраструктуры сетевого общения пользователей интернет-участников открытого и неконтролируемого взаимодействия в медиа-пространстве.

Сокрытие информации в медиа-пространстве обычно производят при помощи стеганографических алгоритмов. Существует несколько задач, для решения которых используют такие алгоритмы, например:

1. Обеспечение тайны переписки (postal privacy):
2. Общение удаленных абонентов, обменивающихся цифровыми массивами информации.
3. Общение удаленных абонентов в открытых сетевых структурах.
4. Достижение скрытности хранимой информации большого объема.

В данной работе представлены основные принципы, на базе которых разрабатываются и функционируют стеганографические алгоритмы.

Понятие стегосистемы

Решение задачи встраивания и выделения сообщений из другой информации выполняет стегосистема. Стегосистема состоит из следующих основных элементов (Рис.1):

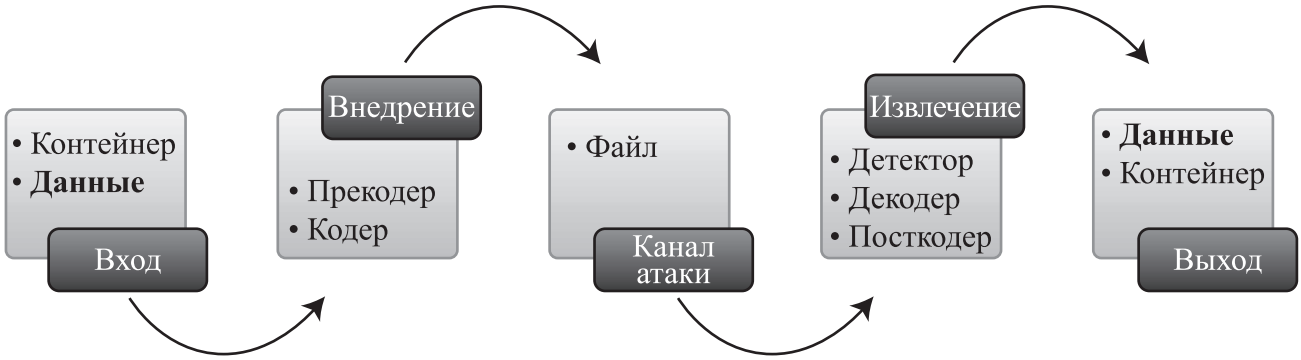

Рис.1.. Основные элементы стегосистемы.

Основными компонентами стегосистемы являются:

1. Контейнер – информационная последовательность, в которой скрываются данные (сообщение).
2. Прекодер – устройство, предназначенное для преобразования скрываемого сообщения к виду, удобному для встраивания в контейнер (обычно на этой стадии сообщение сжимается и шифруется).
3. Кодер (стегокодер) – устройство, предназначенное для осуществления вложения скрытого сообщения в другие данные с учетом их модели.
4. Детектор (стегодетектор) – устройство, предназначенное для определения наличия стегосообщения.
5. Декодер – устройство, восстанавливающее скрытое сообщение из контейнера в сжатом и зашифрованном виде.
6. Посткодер – устройство, приводящее извлеченное сообщение в оригинальное состояние путем распаковки и расшифрования.

Понятие о цифровых водяных знаках

Терминология, встречаемая в литературе для описания алгоритмов внедрения цифровых водяных знаков (ЦВЗ), сильно варьируется [2-5]. Поэтому, на наш взгляд, целесообразно привести наиболее применяемые определения.

ЦВЗ – это специальная метка, встраиваемая в цифровой контент с целью защиты авторских прав и подтверждения целостности самого документа. ЦВЗ можно встраивать в электронные документы любого типа. Наряду с различными изображениями (фотографиями, рисунками, отсканированными бумажными документами и т.д.) встречаются аудиозаписи и видео, несущие внутри себя ЦВЗ. ЦВЗ активно используются при размещении уникальных фотографий, видео, аудиотреков в электронном виде в глобальной сети Интернет.

Результат внедрения ЦВЗ в стеганоконтйнер (также называемое изображение-контейнер) будет называться подписанное изображение. В некоторых стеганоалгоритмах в виде ЦВЗ будет использоваться некоторая уникальная последовательность данных – секретный ключ. Детектор ЦВЗ может однозначно

определить содержит ли изображение внедренный ЦВЗ или нет.

Рассмотрим требования к ЦВЗ наиболее часто упоминаемые в литературе [4, 6]:

1. Скрытность. Внедрение ЦВЗ не должно ухудшать изображение стегоконтейнера. Наличие ЦВЗ не должно быть визуально определимо.
2. Устойчивость. ЦВЗ не должен повреждаться в результате манипуляций со стегоконтейнером, которые могут произойти при его санкционированном использовании, таким как фильтрация, сжатие с потерями, обрезка, распечатка и сканирование, преобразование в другой формат.
3. Защищенность от злонамеренного воздействия. ЦВЗ должен противостоять попыткам удаления его из стегоконтейнера или, по крайней мере, это должно сопровождаться неприемлемым уровнем повреждения изображения самого стегоконтейнера.
4. Общедоступность. Метод внедрения ЦВЗ должен быть широко известен. Криптографический принцип «безопасность через непонятность» здесь не приемлем. Сохранение алгоритма внедрения ЦВЗ в тайне исключит его из стандартах механизмов просмотра изображения и тем самым снизить защиту.
5. Многократное применение. Должна быть возможность многократного применения ЦВЗ. Это необходимо для случаев, когда продукт произведен несколькими производителями и каждый из них имеет свой собственный стандарт ЦВЗ.
6. Расширяемость. Возможность использовать улучшенные версии той же самой технологии внедрения, когда будет доступна большая мощность вычислительной техники.
7. Самосинхронизация. Если доступен только фрагмент стегоконтейнера, полученный в результате обрезки или вращения, ЦВЗ должен по-прежнему детектироваться и читаться.

Следует подчеркнуть, что перечисленные требования не обязательно выполняются в существующих стеганоалгоритмах в полном объеме. Более того, некоторые свойства находятся в явном противоречии друг с другом. Например, требование 1 предполагает, что информация должна встраиваться в области как можно менее значимые, поскольку это произведет наименьшее воздействие на изображение и изменения будут незаметны. В свою очередь требование 2, наоборот, предполагает встраивание ЦВЗ в наиболее значимые области, которые даже при фильтрации или сжатии с потерями не будут затронуты и сохранят без изменений внедренный в них ЦВЗ. Как правило, при разработке стеганоалгоритма авторы делают акцент на определенное свойство или группу свойств.

Удовлетворить всем требованиям, предъявляемым к ЦВЗ непросто, однако существует много компаний предлагающих конкурирующие технологии и соответствующие программы для нанесения (внедрения) ЦВЗ. Все эти программы работают на основе использования шума для создания ЦВЗ - случайных данных, которые существуют в большинстве цифровых файлов. Чтобы распознать ЦВЗ необходима специальная программа для восстановления данных.

Наиболее продвинутой, в маркетинговом отношении, является технология PictureMark фирмы Digimark. PictureMarc представляет собой встраиваемый модуль (plug-in) для основных графических пакетов как, например, Adobe Photoshop и Corel PhotoPaint. Технология допускает достаточно большой диапазон трансформаций с изображениями

с встроенными ЦВЗ. Анализ устойчивости многих систем встраивания ЦВЗ в цифровые изображения показывает, что современные технологии еще не готовы для публичного использования в Internet – существуют очень простые методы удаления ЦВЗ.

Классификация стеганосистем ЦВЗ

Стеганосистемы можно классифицировать по нескольким критериям. Например, в зависимости от того, какая информация требуется детектору для обнаружения ЦВЗ. Стегосистемы ЦВЗ делятся на три класса: открытые, полузакрытые и закрытые системы. Эта классификация приведена в таблице.

1. Watermarking – встраивание цифровых водяных знаков (ЦВЗ);
2. Fingerprinting – встраивание идентификационных номеров;
3. Captioning – встраивание заголовков;
4. Встраивание информации с целью ее скрытой передачи;

ЦВЗ появились в сфере мультимедийных технологий в результате применения в данной области модели защиты от подделки денежных купюр. Вопрос защиты авторских прав актуален и важен, и, поскольку, современные технологии позволяют создавать значительные объемы объектов интеллектуальной собственности за сравнительно небольшие удельные сроки, наличие и применение стандартов и механизмов встраивания ЦВЗ в объекты творчества в автоматическом режиме является принципиальным. В отличие от денежных купюр, на которых водяные знаки видны, объекты мультимедиа (цифровые изображения, видеофайлы, аудиозаписи), как правило, при внедрении ЦВЗ обрабатываются таким образом, чтобы исключить восприятие ЦВЗ человеком по видео и аудио каналам.

Таблица.
Классификация систем встраивания ЦВЗ

		Информация, требуемая детектору		Выход детектора	
		Исходный сигнал	Исходный ЦВЗ	Да/Нет	ЦВЗ
Закрытые	Тип I	+	+	+	-
	Тип II	+	-	-	+
Полузакрытые		-	+	+	-
Открытые		-	-	-	+

На Рис. 2 приведена полная классификация стеганосистем цифровой стеганографии. Как видно из этого рисунка, характеристика каждого стеганографический алгоритма является линейной комбинацией показателей по различным критериям сравнения.

Анализ основных направлений стеганографии

Основными направлениями стеганографии принято считать:

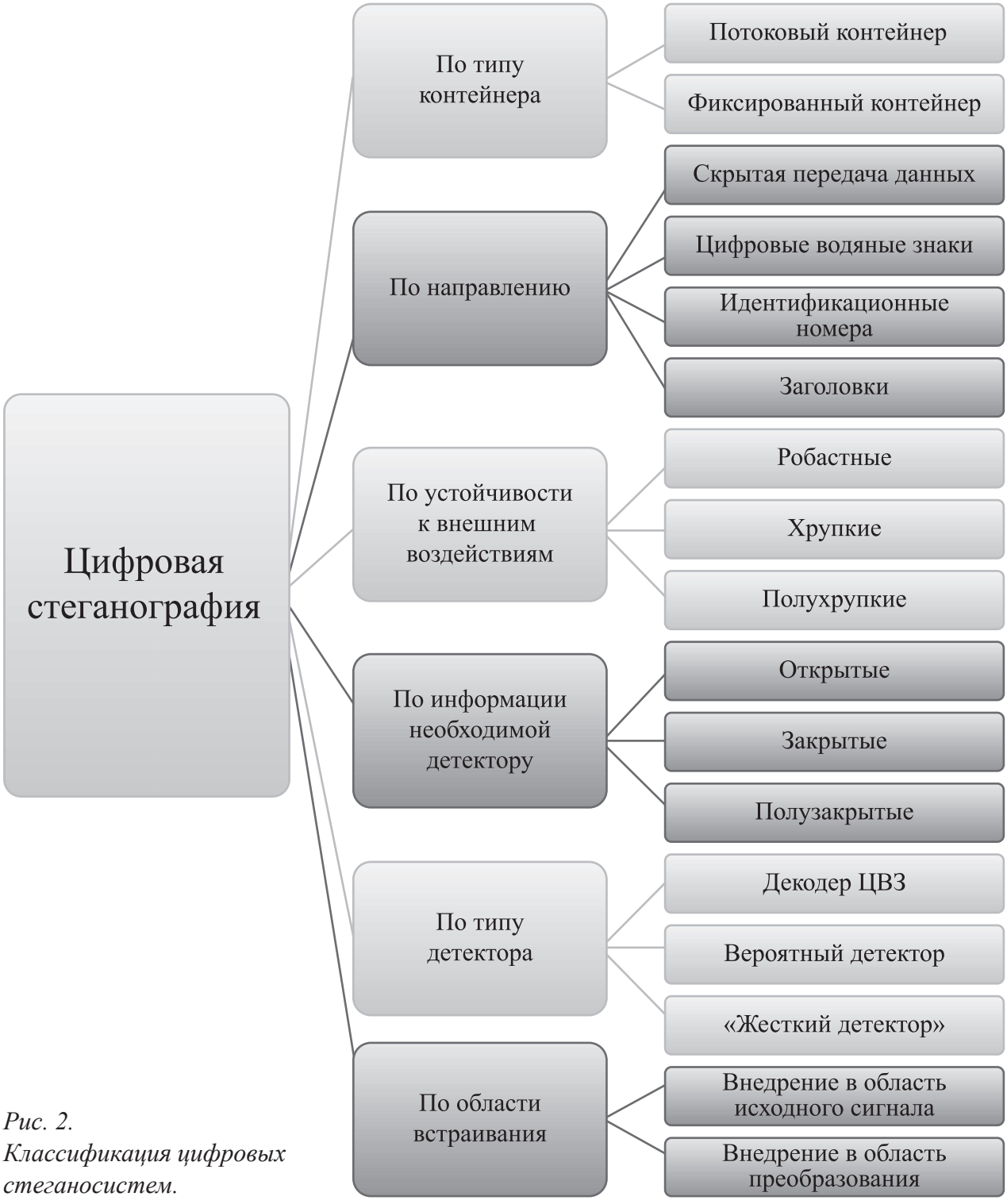

Рис. 2.
Классификация цифровых стеганосистем.

Встраивание идентификационных номеров является вырожденным случаем встраивания ЦВЗ и осуществляется с целью отслеживания дальнейшей судьбы объекта интеллектуальной собственности. Именно по этой причине для каждого экземпляра группы объектов определяется уникальный идентификационный номер, который встраивается в объект с тем, чтобы в будущем иметь представление об истории распространения

каждой отдельной копии. В случае незаконного тиражирования недоверенной стороной будут появляться копии с повторяющимися идентификационными номерами.

Целью встраивания заголовков является категорирование и каталогизация объектов. Это применение стеганографии актуально для библиотек и различных хранилищ, медицинских и образовательных учреждений, где существует множество артефактов, по которым необходимо осуществлять поиск.

Задача сокрытия данных во внешне безобидных контейнерах с целью скрытой передачи не нова, но, вместе с тем, актуальна и сегодня. Существует необходимость защиты переписки и абоненты сети вправе наряду с криптографическими средствами защиты циркулирующей информации использовать и стеганографический подход, чтобы скрыть сам факт переписки. Наиболее существенное отличие постановки задачи скрытой передачи данных от постановки задачи встраивания ЦВЗ состоит в том, что в первом случае нарушитель должен обнаружить скрытое сообщение, тогда как во втором случае о его существовании все знают. Более того, у нарушителя на законных основаниях может иметься устройство обнаружения ЦВЗ.

Анализ стеганоалгоритмов для графических контейнеров

Использование графики в качестве стегоконтейнеров обусловлено следующими причинами:

1. Высокая степень распространения цифровой графики (начиная с любительских фотографий, заканчивая файлами профессиональной графики) на электронных устройствах – носителях информации – личного пользования и в сети интернет.
2. Популярность, очевидность и простота процессов обмена цифровыми фотографиями и опубликования цифровых фотографий в сети интернет.
3. Удобный объем контейнера с точки зрения операций работы с файлами (аудиофайлы и видеофайлы, как правило, в среднем имеют больший объем, чем цифровые изображения).
4. Существование особенностей системы человеческого зрения, не позволяющих визуально определить наличие незначительных изменений контейнера.

Существуют различные форматы изображений и различные подходы к встраиванию данных. Ниже рассмотрены стеганоалгоритмы, работающие с изображениями формата JPEG.

Форматные методы

Форматные методы, по мнению специалистов, не относятся к цифровой стеганографии в чистом виде, поскольку не связаны с цифровой обработкой сигналов [7]. Они основаны на избыточности форматов компьютерных данных, например, структуре файлов, IP-пакетов. Цифровые изображения также являются сигналами, имеющими, однако, «застывший» характер. С этой точки зрения, при работе с алгоритмом, дописывающим в конец файла JPEG байты файла RAR, строго нельзя говорить о цифровой стеганографии изображений, поскольку это не что иное, как форматный метод в компьютерной стеганографии.

Стеганоалгоритмы пространственной области

Алгоритмы данного типа внедряют информацию в области самого изображения. Их преимуществом является то, что для внедрения нет

необходимости выполнять вычисли-тельно громоздкие линейные преобразования изображений. Данные внедряются за счет манипуляций цветовыми составляющими *(r(x,y),b(x,y),g(x,y))* или яркостью $l(x,y) \in \{1,...,L\}$.

Исторически, такие алгоритмы возникли во времена широкого распространения графического формата BMP, в котором подразумевается хранение информации о цветовых составляющих каждой точки изображения. Отличие разновидностей BMP заключается в кодировании цветовых составляющих и, как следствие, в количестве цветов, полутонов и оттенков возможных быть представленными в том, или ином BMP изображении. Наиболее полноцветный формат – BMP24 использует 3 байта для кодирования цвета каждой точки (пикселя). Каждый байт может кодировать 256 оттенков цвета, соответственно 3 байта дают возможность каждому пикселю быть представленным одним из 2563 = 16777216 миллионов цветовых оттенков.

Стеганоалгоритмы области преобразования

В стеганографии наиболее популярны два преобразования [7]:

- Дискретное косинусное преобразование (ДКП).
- Вейвлет-преобразование (ВП).

ДКП используется в алгоритме сжатия JPEG, что является большим стимулом использования ДКП в стеганографии JPEG. ВП, является основой сжатия в алгоритме JPEG 2000.

ДКП может применяться как ко всему изображению в целом, так и к отдельным блокам пикселей изображения. Обычно же контейнер разбивается на блоки размером 8×8 пикселей. ДКП применяется к каждому блоку, в результате чего получаются матрицы коэффициентов ДКП, также размером 8×8 [8]. Коэффициенты обозначаются через $c_b(j, k)$, где b – номер блока, (j, k) – позиция коэффициента внутри блока. Если блок сканируется в зигзагообразном порядке (как это имеет место в JPEG), то коэффициенты обозначаются через $c_{b,j}$. Коэффициент в левом верхнем углу $c_b(0,0)$, обычно называется DC-коэффициентом. Он содержит информацию о яркости всего блока. Остальные коэффициенты называются AC-коэффициентами. Иногда выполняется ДКП всего изображения, а не отдельных блоков.

Рассмотрим процесс внедрения/извлечения информации в области ДКП на примере алгоритма Koch [9]. В данном алгоритме в блок размером 8×8 осуществляется встраивание 1 бита ЦВЗ. Известны две реализации алгоритма: псевдослучайно могут выбираться два или три коэффициента ДКП. Предлагается модификация алгоритма с двумя выбираемыми коэффициентами (s_i).

Встраивание информации осуществляется следующим образом: для передачи бита 0 добиваются того, чтобы разность абсолютных значений коэффициентов была бы больше некоторой положительной величины ε, а для передачи бита 1 эта разность делается меньше некоторой отрицательной величины $-\varepsilon$:

$$|c_b(j_{i,j}, k_{i,1})| - |c_b(j_{i,2}, k_{i,2})| > \varepsilon, \quad \text{если } s_i = 0,$$
$$|c_b(j_{i,j}, k_{i,1})| - |c_b(j_{i,2}, k_{i,2})| < -\varepsilon, \quad \text{если } s_i = 1.$$

Таким образом, исходное изображение искажается за счет внесения изменений в коэффициенты ДКП.

Для чтения ЦВЗ в декодере выполняется та же процедура выбора коэффициентов, и решение о переданном бите принимается согласно правилу:

$$s_i = 0, \text{ если } |c_b(j_{i,j}, k_{i,1})| > |c_b(j_{i,2}, k_{i,2})|$$
$$s_i = 1, \text{ если } |c_b(j_{i,j}, k_{i,1})| < |c_b(j_{i,2}, k_{i,2})|.$$

Заключение

Исследования показали, что область преобразования не подходит для сокрытия больших объемов данных, о которых обычно идет речь при скрытой передаче сообщений в графических контейнерах. Область преобразования подходит для встраивания ЦВЗ, представляющих собой короткие последовательности байтов. Принципиальным является и набор ограничений, применяемых к стегоконтейнеру.

Выводы:

1. Вопросы скрытой передачи данных как направления стеганографии недостаточно освещены. Существующие стеганографические алгоритмы в большей степени ориентированы на работу с ЦВЗ.
2. Стеганоалгоритмы, работающие с пространственной областью изображения основаны на визуальной избыточности зрительно-воспринимаемой информации и на данный момент не являются столь популярными, как стеганоалгоритмы области преобразования, за счет широкого распространения формата JPEG, в котором цветовые или яркостные составляющие точек скрыты за областью преобразования.
3. Область преобразования более подходит для сокрытия небольшого количества информации, например ЦВЗ, за счет ограниченного числа потенциальных мест для встраивания.
4. Для сокрытия больших объемов данных более подходит пространственная область изображения, однако для файлового формата JPEG данная область скрыта за областью преобразования.

Библиография:

1. Сидоркина И.Г., Коробейников А.Г, Кудрин П.А. Алгоритм распознавания трехмерных изображений с высокой детализацией// Вестник МарГТУ, 2 (9), 2010 г., стр. 91-99.
2. Артёзин Б.В Стеганография // Журнал «Защита информации. Конфедент». 1996. № 4. – С. 47-50.
3. Грибунин В.Г., Оконов И.Н., Туринцев И.В. Цифровая стеганография. – М.:Солон-Пресс, 2002. 272 с.
4. Husrev T. Sencar, Mahalinggam Pamkumar, Data Hiding Fundamentals And Applications. Content Security In Digital Multimedia/ ELSEVIER science and technology books, 2004. 364 p.
5. Petitcolas F., Anderson R.J., Kuhn M.G. Information Hiding – A Survey // Proceedings IEEE, Special Issue on Identification and Protection of Multimedia Information. 1999. Vol. 87. №. 7. P. 1069-1078.
6. W. Bender, D. Gruhl, N. Morimoto, A. Lu, Tehniques for data Hiding/ IBM Systems Journal, 35 (3&4): pp. 313-336, 1996.
7. Коробейников А.Г., Кувшинов С.С., Лейман А.В., Блинов С.Ю., Нестеров С.И. Разработка стеганоалгоритма на базе форматных и пространственных принципов сокрытия данных//Научно-технический вестник информационных технологий, механики и оптики – СПб: СПБНИУ ИТМО, 2012, 1(77)– с.116 – 119.
8. Коробейников А.Г., Прохожев Н.Н., Михайличенко О.В., Хоанг З. Выбор коэффициентов матрицы дискрет¬нокосинусного преобразования при построении стеганографических систем//Вестник компьютерных и инфор¬мационных технологий. – 2008. – № 11. – С. 12–17.
9. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. – Киев: МК-Пресс, 2006. – 288 с.

References (transliteration):

1. Cidorkina I.G., Korobeynikov A.G, Kudrin P.A. Algoritm raspoznavaniya trekhmernykh izobrazheniy s vysokoy detalizatsiey// Vestnik MarGTU, 2 (9), 2010 g., str. 91-99.
2. Artezin B.V Steganografiya // Zhurnal «Zashchita informatsii. Konfedent». 1996. № 4. – S. 47-50.
3. Gribunin V.G., Okonov I.N., Turintsev I.V. Tsifrovaya steganografiya. – M.:Solon-Press, 2002. 272 s.
4. Husrev T. Sencar, Mahalinggam Pamkumar, Data Hiding Fundamentals And Applications. Content Security In Digital Multimedia/ ELSEVIER science and technology books, 2004. 364 p.
5. Petitcolas F., Anderson R.J., Kuhn M.G. Information Hiding – A Survey // Proceedings IEEE, Special Issue on Identification and Protection of Multimedia Information. 1999. Vol. 87. №. 7. P. 1069-1078.
6. W. Bender, D. Gruhl, N. Morimoto, A. Lu, Tehniques for data Hiding/ IBM Systems Journal, 35 (3&4): pp. 313-336, 1996.
7. Korobeynikov A.G., Kuvshinov S.S., Leyman A.V., Blinov S.Yu., Nesterov S.I. Razrabotka steganoalgoritma na baze formatnykh i prostranstvennykh printsipov sokrytiya dannykh//Nauchno-tekhnicheskiy vestnik informatsionnykh tekhnologiy, mekhaniki i optiki – SPb: SPBNIU ITMO, 2012, 1(77)– s.116 – 119.
8. Korobeynikov A.G., Prokhozhev N.N., Mikhaylichenko O.V., Khoang Z. Vybor koeffitsientov matritsy diskret¬no-kosinusnogo preobrazovaniya pri postroenii steganograficheskikh sistem//Vestnik komp'yuternykh i infor¬matsionnykh tekhnologiy. – 2008. – № 11. – S. 12–17.
9. Konakhovich G.F., Puzyrenko A.Yu. Komp'yuternaya steganografiya. Teoriya i praktika. – Kiev: MK-Press, 2006. – 288 s.