ВЕЙВЛЕТЫ В СТЕГАНОГРАФИИ

Вадим Грибунин

В последние годы появилась и оформилось новая научная дисциплина, находящаяся на стыке цифровой обработки сигналов, теории связи и криптографии – цифровая стеганография. Под цифровой стеганографией понимается скрытие одних данных в других методами ЦОС. Например, можно «упрятать» картинку в картинке, речь в речи, речь в изображении и т.д.

Можно выделить две причины популярности исследований в области стеганографии в настоящее время: ограничение на использование криптосредств в ряде стран мира и появление проблемы защиты прав собственности на информацию, представленную в цифровом виде. Первая причина повлекла за собой большое количество исследований в духе классической стеганографии (то есть скрытия факта передачи информации), вторая – еще более многочисленные работы в области так называемых водяных знаков. Цифровой водяной знак (ЦВЗ) – специальная метка, незаметно внедряемая в изображение или другой сигнал с целью тем или иным образом контролировать его использование.

Название этот метод получил от всем известного способа защиты ценных бумаг, в том числе и денег, от подделки. В отличие от обычных водяных знаков ЦВЗ могут быть не только видимыми, но и (как правило) невидимыми. Невидимые ЦВЗ анализируются специальным декодером, который выносит решение об их релевантности. ЦВЗ могут содержать некоторый аутентичный код, информацию о собственнике, либо какую-нибудь управляющую информацию. Наиболее подходящими объектами для защиты при помощи ЦВЗ являются неподвижные изображения, файлы аудио и видеоданных.

Здесь необходимо сделать ряд замечаний.

Во-первых, так как цифровая стеганография является молодой наукой, ее терминология не устоялась. Так, некоторые исследователи понимают под стеганографией только скрытую передачу данных. Другие - относят к стеганографии, например, метеорную радиосвязь, радиосвязь с псевдослучайной перестройкой радиочастоты, широкополосную радиосвязь. На наш взгляд, неформальное определение того, что такое цифровая стеганография могло бы выглядеть следующим образом: «наука о незаметном и надежном скрытии одних битовых последовательностей в других». Под это определение как раз подпадают все четыре вышеприведенных направления скрытия данных, а приложения радиосвязи - нет. Кроме того, в определении содержится два главных требования к стеганографическому кодированию: незаметность и надежность, или устойчивость к различного рода искажениям.

Во-вторых, как бы ни были различны направления стеганографии, предъявляемые ими требования во многом совпадают, как будет показано далее. Наиболее существенное отличие методов скрытой передачи данных от методов ЦВЗ состоит в том, что в первом случае задача нарушителя заключается в обнаружении скрытого сообщения, тогда как во втором случае о его существовании все знают. Более того, у нарушителя на законных основаниях может иметься устройство обнаружения ЦВЗ (например, в составе DVD-проигрывателя).

Прочтите еще раз наше определение цифровой стеганографии. Слово «незаметном» подразумевает обязательное включение человека в систему стеганографической передачи данных. Человек здесь может рассматриваться как дополнительный приемник данных, предъявляющий к системе передачи достаточно трудно формализуемые требования.

Задачу встраивания и выделения сообщений из другой информации выполняет стегосистема. Стегосистема состоит из следующих основных элементов:

- прекодер – устройство, предназначенное для преобразования скрываемого сообщения к виду, удобному для встраивания в сигнал;
- стегокодер – устройство, предназначенное для осуществления вложения скрытого сообщения в другую информацию;
- стегодетектор – устройство, предназначенное для определения наличия и/или выделения сообщения;
- декодер – устройство, восстанавливающее скрытое сообщение. Этот узел может отсутствовать, как будет пояснено далее.

Прежде, чем осуществить вложение ЦВЗ в контейнер, ЦВЗ должен быть преобразован к некоторому подходящему виду. Например, если в качестве контейнера выступает изображение, то и последовательность ЦВЗ зачастую представляется как двумерный массив бит. Для того, чтобы повысить устойчивость ЦВЗ к искажениям нередко выполняют его помехоустойчивое кодирование, либо применяют широкополосные сигналы. Предварительную обработку скрытого сообщения выполняет прекодер. В качестве важнейшей предварительной обработки ЦВЗ (а также и контейнера) назовем вычисление его обобщенного преобразования Фурье. Это позволяет осуществить встраивание ЦВЗ в спектральной области, что значительно повышает его устойчивость к искажениям. Предварительная обработка часто выполняется с использованием ключа K. Далее ЦВЗ «вкладывается» в контейнер. Этот процесс возможен благодаря особенностям системы восприятия человека. Хорошо известно, например, что изображения обладают большой психовизуальной избыточностью. Глаз человека подобен низкочастотному фильтру, пропускающему мелкие детали. Особенно незаметны искажения в высокочастотной области изображений. Эти особенности человеческого зрения используются при разработке алгоритмов сжатия изображений и видео.

Процесс вложения стего также должен учитывать свойства системы восприятия человека. Стеганография использует имеющуюся в сигналах психовизуальную избыточность, но другим, чем при сжатии данных образом. Приведем простой пример. Рассмотрим полутоновое изображение с 256 градациями серого, то есть с удельной скоростью кодирования 8 бит/пиксел. Хорошо известно, что глаз человека не способен заметить изменение младшего значащего бита. Еще в 1989 году был получен патент на способ скрытого вложения информации в изображение путем модификации младшего значащего бита. В данном случае детектор стего анализирует только значение этого бита для каждого пиксела, а глаз человека, напротив, воспринимает только старшие 7 бит. Данный метод прост в реализации и эффективен, но не удовлетворяет некоторым важным требованиям к ЦВЗ, как будет показано далее.

В большинстве стегосистем для вложения и выделения ЦВЗ используется ключ. Ключ может быть предназначен для узкого круга лиц или же быть общедоступным. Например, ключ должен содержаться во всех DVD-плейерах, чтобы они могли прочесть содержащиеся на дисках ЦВЗ. Иногда по аналогии с криптографией стегосистемы делят на два класса: с открытым ключом и с секретным ключом. На наш взгляд, аналогия неверна, так как понятие открытого ключа в данном случае в корне различно. Не существует, насколько известно, стегосистемы, в которой бы при выделении ЦВЗ требовалась другая информация, чем при его вложении. Хотя и не доказана гипотеза о невозможности существования подобной системы. В системе с общедоступным ключом достаточно сложно противостоять возможным атакам со стороны злоумышленников. В самом деле, в данном случае нарушителю точно известен ключ и месторасположение ЦВЗ, а также его значение.

В стегодетекторе происходит обнаружение ЦВЗ в (возможно измененном) защищенном ЦВЗ изображении. Это изменение может быть обусловлено влиянием ошибок в канале связи, операций обработки сигнала, преднамеренных атак нарушителей. Во многих моделях стегосистем сигнал-контейнер рассматривается как аддитивный шум. Тогда задача обнаружения и выделения стего является классической для теории связи. Однако такой подход не учитывает двух факторов: неслучайного характера сигнала контейнера и требований по сохранению его качества. Эти моменты не встречаются в известной теории обнаружения и выделения сигналов на фоне аддитивного шума. Их учет позволит построить более эффективные стегосистемы.

Различают стегодетекторы, предназначенные для обнаружения факта наличия ЦВЗ и устройства, предназначенные для выделения этого ЦВЗ (стегодекодеры). В первом случае возможны детекторы с жесткими (да/нет) или мягкими решениями. Для вынесения решения о наличии/отсутствии ЦВЗ удобно использовать такие меры, как расстояние по Хэммингу, либо взаимную корреляцию между имеющимся сигналом и оригиналом (при наличии последнего, разумеется). А что делать, если у нас нет исходного сигнала? Тогда в дело вступают более тонкие статистические методы, основанные на построении моделей исследуемого класса сигналов.

В зависимости от того, какая информация требуется детектору для обнаружения ЦВЗ, стегосистемы делятся на три класса: открытые, полузакрытые и закрытые системы. Классификация представлена в Таблице 1-1.

Таблица 1-1

		Что требуется детектору		Выход детектора	
		Исх.изображение	Исходный ЦВЗ	Да/Нет	ЦВЗ
Закрытые	Тип I	+	+	+	-
	Тип II	+	-	-	+
Полузакрытые		-	+	+	-
Открытые		-	-	-	+

Наибольшее применение имеют открытые стегосистемы ЦВЗ, которые аналогичны системам скрытой передачи данных. Наибольшую устойчивость по отношению к внешним воздействиям имеют закрытые стегосистемы I типа.

Информационная последовательность, в которой прячется сообщение, называется контейнером. До стегокодера – это пустой контейнер, после него – заполненный контейнер, или стего. Стего должен быть визуально неотличим от пустого контейнера. Различают два основных типа контейнеров: потоковый и фиксированный.

Потоковый контейнер представляет собой непрерывно следующую последовательность бит. Сообщение вкладывается в него в реальном масштабе времени, так что в кодере неизвестно заранее, хватит ли размеров контейнера для передачи всего сообщения. В один контейнер большого размера может быть встроено и несколько сообщений. Интервалы между встраиваемыми битами определяются генератором псевдослучайной последовательности с равномерным распределением интервалов между отсчетами. Основная трудность заключается в осуществлении синхронизации, определении начала и конца последовательности. Если в данных контейнера имеются биты синхронизации, заголовки пакетов и т.д., то скрываемая информация может идти сразу после них. Трудность обеспечения синхронизации превращается в достоинство с точки зрения обеспечения скрытности передачи. Кроме того, потоковый контейнер имеет большое практическое значение: представьте себе, например, стегоприставку к обычному телефону. Не случайно, что работ, посвященных использованию потокового контейнера практически не встречается.

У фиксированного контейнера размеры и характеристики заранее известны. Это позволяет осуществлять вложение данных оптимальном в некотором смысле словом.

Контейнер может быть выбранным, случайным или навязанным. Выбранный контейнер зависит от встраиваемого сообщения, а в предельном случае является его функцией. Этот тип контейнера больше характерен для стеганографии. Навязанный контейнер может появиться в сценарии, когда лицо, предоставляющее контейнер, подозревает о возможной скрытой переписке и желает предотвратить ее. На практике же чаще всего сталкиваются со случайным контейнером.

Встраивание сообщения в контейнер может производиться при помощи ключа, одного или нескольких. Ключ - псевдослучайная последовательность бит, порождаемая генератором, удовлетворяющим определенным требованиям. В качестве основы генератора может использоваться, например, линейный рекуррентный регистр. Тогда адресатам для обеспечения связи может сообщаться начальное заполнение этого регистра. Надо отметить, что метод случайного выбора величины интервала между встраиваемыми битами не особенно хорош. Причин этого две. Во-первых, скрытые данные должны быть распределены по всему изображению. Поэтому, равномерное распределение длин интервалов (от наименьшего до наибольшего) может быть достигнуто лишь приближенно, так как мы должны быть уверены в том, что все сообщение встроено. Во-вторых, длины интервалов шума распределены не по равномерному, а по экспоненциальному закону. Генератор же ПСП с экспоненциально распределенными интервалами сложен в реализации.

ЦВЗ могут быть трех типов: робастные, хрупкие и полухрупкие (semifragile). Под робастностью понимается устойчивость ЦВЗ к различного рода воздействиям на стего. Это – наиболее часто встречающийся вид ЦВЗ.

Хрупкие ЦВЗ разрушаются при незначительной модификации заполненного контейнера. Они применяются для аутентификации сигналов. Отличие от средств электронной цифровой подписи заключается в том, что хрупкие ЦВЗ все же допускают некоторую модификацию контента. Это важно для защиты мультимедийной информации, так как законный пользователь может, например, пожелать сжать изображение. Другое отличие заключается в том, что хрупкие ЦВЗ должны не только отразить факт модификации контейнера, но также вид и местоположение этого изменения.

Полухрупкие ЦВЗ устойчивы по отношению к одним воздействиям и неустойчивы по отношению к другим. Вообще говоря, все ЦВЗ могут быть отнесены к этому типу. Однако полухрупкие ЦВЗ специально проектируются так, чтобы быть неустойчивыми по отношению к определенного рода операциям. На рисунке представлена классификация систем цифровой стеганографии.

Стегосистема образует стегоканал, по которому передается заполненный контейнер. Этот канал считается подверженным воздействиям со стороны нарушителей. Следуя Симмонсу, в стеганографии обычно рассматривается такая постановка задачи («проблема заключенных»). Двое заключенных, Алиса и Боб желают конфиденциально обмениваться сообщениями, несмотря на то, что канал связи между ними контролирует охранник Вилли. Для того, чтобы тайный обмен сообщениями был возможен предполагается, что Алиса и Боб имеют некоторый известный обоим секретный ключ. Действия Вилли могут заключаться не только в попытке обнаружения скрытого канала связи, но и в разрушении передаваемых сообщений, а также их модификации и создании новых, ложных. Соответственно, можно выделить три типа нарушителей, которым должна противостоять стегосистема: Наблюдатель, Разрушитель и Созидатель (или пассивный, активный и злоумышленный нарушители). Наблюдатель может быть лишь в стегосистемах скрытой передачи данных. Для систем ЦВЗ характерны Разрушители и Созидатели.

Статья Симмонса, как он сам написал впоследствии была вызвана желанием привлечь внимание научной общественности к закрытой в то время проблеме, связанной с контролем над ядерным оружием. Согласно Договору ОСВ СССР и США должны были разместить некие датчики на стратегических ракетах друг друга. Эти датчики должны были передавать информацию о том, не подсоединена ли к ним ядерная боеголовка. Проблема, которой занимался Симмонс, заключалась в том, чтобы не допустить передачи како-либо другой информации этими датчиками, например, о местоположении ракет. Определение факта наличия скрытой информации – главная задача стегоанализа.

Для того, чтобы стегосистема была надежной, необходимо выполнение при ее проектировании ряда требований.

- Безопасность системы должна полностью определяться секретностью ключа. Это означает, что нарушитель может полностью знать все алгоритмы работы стегосистемы, и это не даст ему никакой дополнительной информации о наличии или отсутствии сообщения в данном контейнере.
- Знание нарушителем факта наличия сообщения в каком-либо контейнере не должно помочь ему при обнаружении сообщений в других контейнерах.
- Заполненный контейнер должен быть визуально неотличим от незаполненного. Для удовлетворения этого требования надо, казалось бы, внедрять скрытое сообщение в визуально незначимые области сигнала. Однако, эти же области используют и алгоритмы сжатия. Поэтому, если изображение будет в дальнейшем подвергаться сжатию, то скрытое сообщение может разрушиться. Следовательно, биты должны встраиваться в визуально значимые области, а относительная незаметность может быть достигнута за счет использования специальных методов, например, модуляции с расширением спектра.
- Стегосистема должна иметь низкую вероятность ложного обнаружения стего в сигнале, его не содержащем. В некоторых приложениях такое обнаружение может привести к серьезным последствиям. Например, ложное обнаружение ЦВЗ на DVD-диске может вызвать отказ от его воспроизведения плейером.
- Должна обеспечиваться требуемая пропускная способность.
- Стегосистема должна иметь приемлемую вычислительную сложность. При этом возможна асимметричная система ЦВЗ, то есть сложный стегокодер и простой стегодекодер.

К ЦВЗ предъявляются следующие требования.

- ЦВЗ должен легко (вычислительно) извлекаться законным пользователем.
- ЦВЗ должен быть устойчивым либо неустойчивым к преднамеренным и случайным воздействиям (в зависимости о приложения). Если ЦВЗ используется для подтверждения подлинности, то любое изменение контейнера должно приводить к невозможности извлечения ЦВЗ (хрупкий ЦВЗ). Если же ЦВЗ содержит идентификационный код, логотип фирмы и т.п., то он напротив должен быть извлечен при максимальных искажениях контейнера, конечно, не приводящих к существенным искажениям исходного сигнала. Например, у изображения могут быть отредактированы цветовая гамма или яркость, у аудиозаписи – усилено звучание низких тонов и т.д. Кроме того, стего должно быть робастно по отношению к аффинным преобразованиям изображения, то есть поворотам, масштабированию. При этом некоторые авторы подчеркивают, что надо различать устойчивость самого ЦВЗ и способность декодера верно его обнаружить. Скажем, при повороте

изображения стего не разрушится, а декодер может оказаться неспособным выделить его. Существуют приложения, когда ЦВЗ должно быть устойчивым по отношению к одним преобразованиям и неустойчивым по отношению к другим. Например, может быть разрешено копирование документа (ксерокс, сканер), но наложен запрет на внесение в него каких-либо изменений.

- Должна иметься возможность добавления к стегоконтейнеру дополнительных ЦВЗ. Например, на DVD-диске имеется метка о допустимости однократного копирования. После осуществления такого копирования необходимо добавить метку о запрете дальнейшего копирования. Можно было бы, конечно, удалить первый ЦВЗ и записать на его место второй. Однако, это противоречит предположению о трудноудалимости ЦВЗ. Лучшим выходом является добавление еще одного ЦВЗ, после которого первый не будет приниматься во внимание. Однако, наличие нескольких ЦВЗ на одном сообщении может облегчить атаку со стороны нарушителя, если не предпринять специальных мер.

В настоящее время технология ЦВЗ находится в самой начальной стадии своего развития. Как показывает практика, должно пройти лет 10-20 для того, чтобы новый криптографический метод широко использовался в обществе. Одной из проблем ЦВЗ является многообразие требований к ним, в зависимости от приложения. Рассмотрим подробнее основные области применения ЦВЗ.

Вначале рассмотрим проблему пиратства, или неограниченного неавторизованного копирования. Алиса продает свою мультимедийную информацию Питеру. Хотя информация могла быть зашифрована во время передачи, ничто не помешает Питеру заняться ее копированием после расшифровки. Следовательно, в данном случае требуется дополнительный уровень защиты от копирования.

Используемые обычно средства аутентификации (цифровая подпись) не совсем подходят для защиты прав на мультимедиа-информацию. Дело в том, что сообщение, снабженное электронной цифровой подписью, должно храниться и передаваться абсолютно точно, «бит в бит». Мультимедиа-информация же может незначительно искажаться как при хранении (за счет сжатия), так и при передаче (влияние одиночных или пакетных ошибок в канале связи). При этом ее качество остается допустимым для пользователя, но цифровая подпись работать не будет. Получатель не сможет отличить истинное, хотя и несколько искаженное сообщение, от ложного. Кроме того, мультимедиа-информация может быть преобразована из одного формата в другой. При этом традиционные средства защиты целостности работать также не будут. Можно сказать, что ЦВЗ защищают именно содержимое аудио-, видеосообщения, а не его цифровое представление.

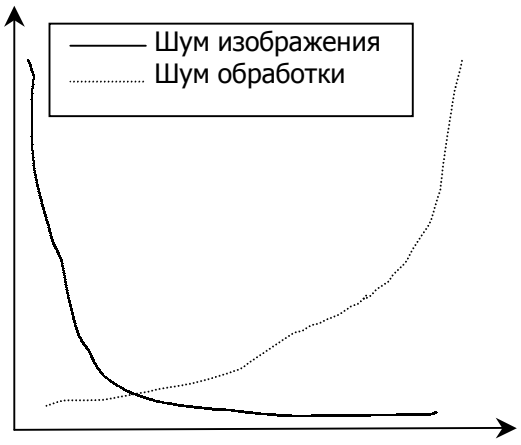
Применение ЦВЗ не ограничивается приложениями безопасности информации. Основные области использования технологии ЦВЗ могут быть объединены в четыре группы: защита от копирования, скрытая аннотация документов, доказательство аутентичности информации и скрытая связь.

Популярность мультимедиа-технологий вызвало множество исследований, связанных с разработкой алгоритмов ЦВЗ для использования в стандартах MP3, MPEG-4, JPEG2000, защиты DVD дисков от копирования.

В большинстве методов скрытия данных в изображениях используется та или иная декомпозиция изображения -контейнера. Среди всех линейных ортогональных преобразований наибольшую популярность в стеганографии получили вейвлет-преобразование и ДКП, что отчасти объясняется их успешным применением при сжатии изображений. Кроме того, желательно применять для скрытия данных то же преобразование изображения, как и то, которому оно подвергнется при возможном дальнейшем сжатии. В стандарте JPEG используется ДКП, а в JPEG2000 – вейвлет-преобразование. Стегоалгоритм может быть весьма робастным к дальнейшей компрессии изображения, если он будет учитывать особенности алгоритма сжатия. При этом, конечно стегоалгоритм, использующий ДКП, вовсе не обязательно будет робастным по отношению к вейвлетному алгоритму сжатию. Стегоалгоритм, использующий вейвлеты, может быть неробастным к сжатию с применением вейвлетов. Еще большие трудности с выбором преобразования при скрытии данных в видеопоследовательности. Причина заключается в том, что при сжатии видео основную роль играет кодирование векторов компенсации движения, а не только неподвижного кадра. Робастный стегоалгоритм должен каким-то образом учитывать это.

Возникает следующий вопрос: существует ли робастное преобразование, независимое от применяемого далее алгоритма сжатия? M.Ramkumar`ом с позиций теории информации рассмотрены различные ортонормальные преобразования, такие как ДПФ, ДКП, Хартли, субполосное преобразование.

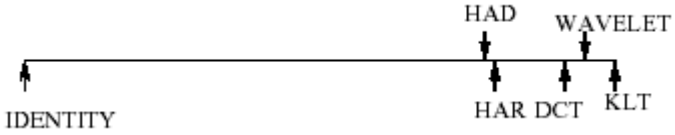
Реальные изображения вовсе не являются случайным процессом с равномерно распределенными значениями величин. Хорошо известно, и это используется в алгоритмах сжатия, что большая часть энергии изображений сосредоточена в низкочастотной части спектра. Отсюда и потребность в осуществлении декомпозиции изображения на субполосы. Теперь стегосообщение должно добавляться к субполосам изображения. Низкочастотные субполосы содержат подавляющую часть энергии изображения и, следовательно, носят шумовой характер. Высокочастотные субполосы наиболее подвержены воздействию со стороны различных алгоритмов обработки, будь то сжатие или НЧ фильтрация. Таким образом, для вложения сообщения наиболее подходящими кандидатами являются среднечастотные субполосы спектра изображения. Типичное распределение шума изображения и обработки по спектру частоты показано на рисунке.



Шум обработки появляется в результате квантования коэффициентов трансформанты. Значение этого шума легко получить, скажем, для пары ДКП – JPEG, если известны таблицы квантования. Однако, например, в случае преобразования Адамара один коэффициент ДКП будет влиять на несколько коэффициентов Адамара. Хотелось бы иметь более общее определение шума обработки. Его можно рассматривать как уменьшение корреляции между коэффициентами трансформанты исходного изображения и квантованными коэффициентами. Например, при высоких степенях сжатия может возникнуть ситуация, когда будут отброшены целые субполосы. То есть дисперсия шума в этих субполосах, вообще говоря, бесконечна. Налицо уменьшение корреляции между коэффициентами субполосы до квантования и после. Конечно для получения приемлемых результатов необходимо усреднить значение шума обработки по многим изображениям.

Выбор значения визуального порога основывается на учете свойств системы человеческого зрения. Известно, что шум в ВЧ областях изображения более приемлем, чем в НЧ областях. Можно ввести некоторые взвешивающие коэффициенты, $\upsilon_j^2 = K\sigma_j^{2\alpha}$, где $K << \sigma_j$ и $0 \le \alpha \le 1$. Случаю, когда $\alpha = 0$ соответствует равномерное распределение стего по всем субполосам, случаю $\alpha = 1$ соответствует распределение стего в соответствии с дисперсиями субполос. После некоторых упрощений можно получить выражение для пропускной способности: $C = \frac{MN}{2L}\log_2\left(1+\sum_{j=1}^{L}\frac{K}{\sigma_j^{2(1-\alpha)}}\right)$. Как видно из этого выражения, при $\alpha = 1$ декомпозиция никак не будет влиять на пропускную способность стегоканала. Тем не менее, при $\alpha < 1$ вид преобразования влияет. Таким образом, пропускная способность возрастает за счет того, что в области с низкой дисперсией (высокочастотные) добавляется относительно больше энергии стегосигнала.

Ramkumar`ом были произведены многочисленные эксперименты, которые позволяют дать определенные рекомендации по выбору преобразования для стеганографии. Преобразования можно упорядочить по достигаемым выигрышам от кодирования (см. рис.).



Наибольший выигрыш дает преобразование Карунена-Лоэва, наименьший – разложение по базису единичного импульса (то есть отсутствие преобразования). Преобразования, имеющие высокие значения выигрыша от кодирования, такие как ДКП, вейвлет-преобразование, характеризуются резко неравномерным распределением дисперсий коэффициентов субполос. Высокочастотные субполосы не подходят для вложения из-за большого шума обработки, а низкочастотные – из-за высокого шума изображения. Поэтому приходится ограничиваться среднечастотными полосами, в которых шум изображения примерно равен шуму обработки. Так как таких полос немного, то пропускная способность стегоканала невелика. В случае применения преобразования с более низким выигрышем от кодирования, например, Адамара или Фурье, имеется больше блоков, в которых шум изображения примерно равен шуму обработки. Следовательно, и пропускная способность выше.

Эффективность применения вейвлет-преобразования и ДКП для сжатия изображений объясняется тем, что они хорошо моделируют процесс обработки изображения в системе зрения человека, отделяют «значимые» детали от «незначимых». Значит, их более це лесообразно применять в случае активного нарушителя. В самом деле, модификация значимых коэффициентов может привести к неприемлемому искажению изображения. При применении преобразования с низкими значениями выигрыша от кодирования существует опасность нарушения вложения, так как коэффициенты преобразования менее чувствительны к модификациям. Однако, существует большая гибкость в выборе преобразования. И если преобразование неизвестно нарушителю (хотя учет этого момента и противоречит принципу Керхгофа), то модификация стего будет затруднена.

В настоящее время в мире предложено огромное количество алгоритмов незаметного встраивания информации в мультимедийные сигналы с использованием вейвлет-преобразования. Ссылки на несколько дипломов и диссертаций, доступных в Сети, мы привели на нашем сайте по адресу: http://www.autex.spb.ru/wavelet/