

УДК 519.25

Моделирование средств стеганографической защиты проектной документации, продуцируемой в САПР

*Логунова А.О., студент
Россия, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Системы автоматизированного проектирования»*

*Научный руководитель: **Волосатова Т.М.**, к.т.н., доцент,
Россия, г. Москва, МГТУ им. Н.Э. Баумана
bauman@bmstu.ru*

Введение

Данная работа посвящена разработке комбинированного метода сокрытия данных, реализующего синтез цифровой голограммы Фурье на основе дискретного косинусного преобразования и алгоритма на основе квантования, а так же исследованию эффективности его использования при кодировании проектной документации.

1. Постановка задачи

Стеганография – это расширяемая совокупность методов и средств передачи (хранения) скрытой информации, при которых скрытый канал организуется на базе и внутри открытого канала с использованием особенностей восприятия информации.

При проведении анализа принято считать, что основными стеганографическими понятиями являются сообщение и контейнер.

Контейнером будем называть несекретные данные, используемые для сокрытия сообщений. Сообщением будем называть секретные данные, наличие которых в контейнере необходимо скрыть. Ключом будем называть секретную информацию, известную только законному пользователю.

В данной работе сообщением будет являться модифицированное изображение, полученное с помощью алгоритма на основе квантования. Ключом будут являться параметры, с помощью которых будет восстанавливаться изображение. Контейнером будет являться изображение, в которое будет встроено сообщение.

2. Алгоритм на основе квантования

Под квантованием понимается процесс сопоставления большого множества значений с некоторым конечным множеством чисел, при этом происходит уменьшение объема информации за счет ее искажения. Квантование находит применение в алгоритмах

сжатия с потерями. Различают скалярное и векторное квантование. При векторном квантовании, в отличие от скалярного, происходит отображение не отдельно взятого отсчета, а их совокупности – вектора, кроме того векторное квантование эффективнее скалярного по степени сжатия (обладает большей сложностью).

В кодере квантователя вся область значений исходного множества делится на интервалы, и в каждом интервале выбирается число его представляющее. Это число есть кодовое слово квантователя и обычно бывает центроидом интервала квантования. Множество кодовых слов называется кодовой книгой. Все значения, попавшие в данный интервал, заменяются в кодере на соответствующее кодовое слово. В декодере принятому числу сопоставляется некоторое значение. Интервал квантования обычно называют шагом квантователя. Встраивание информации с применением квантования относится к нелинейным методам.

Передаваемое сообщение имеет ограниченную энергию для выполнения требования его незаметности. Помехами являются исходный сигнал и шум обработки. Кодеру исходный сигнал известен, декодер должен извлечь ЦВЗ без знания обеих составляющих помех. Существуют многочисленные способы, направленные на борьбу с помехами, заключающиеся в применении различных структурированных квантователей.

Наиболее предпочтительно внедрение информации в спектральную область изображения. Если при этом используются линейные методы, то встраивание ЦВЗ производят в средние полосы частот (энергия изображения сосредоточена, в основном, в низкочастотной (НЧ) области, значит, в детекторе ЦВЗ в этой области наблюдается сильный шум самого сигнала). В высокочастотных (ВЧ) областях большую величину имеет шум обработки, например, сжатия. В отличие от линейных, нелинейные схемы встраивания информации могут использовать НЧ области, так как мощность внедряемого ЦВЗ не зависит от амплитуды коэффициентов (для малой и большой амплитуды они обрабатываются одинаково).

В данной работе применялось встраивание на основе смешанного алгоритма скалярного и векторного квантования.

3. Голограмма Фурье

3.1. Цифровая Фурье - голография

В реализуемом методе, основанном на применении Фурье – голограммы заложены два этапа – внедрение в контейнер зашифрованных данных, а затем получение цифрового голографического изображения. Известно, что в самом общем случае формирование голограммы – это своеобразная модуляция голографируемого объекта.

Вне зависимости от того, в какой области, пространственной или частотной, выполняется модуляция изображения, в основе этих методов лежит интерференция между волновым полем, рассеянным ЦВЗ и пространственной несущей. Здесь проявляется известное свойство преобразования Фурье, которое характеризуется сдвигом спектра сигнала при умножении сигнала на гармоническое колебание. Используя преобразование Фурье объектов, имеющих сдвиг в частотной плоскости относительно начала координат, получаем интерференцию волнового поля, рассеянного объектом, с опорным волновым пучком, то есть комплексную голограмму. Процесс восстановления объекта сопровождается появлением действительного и мнимого изображения. Для моделирования голографических процессов применяется способ преобразования Фурье простых объектов, имеющих некоторое смещение относительно начала координат. Такие голограммы получили название цифровых Фурье - голограмм.

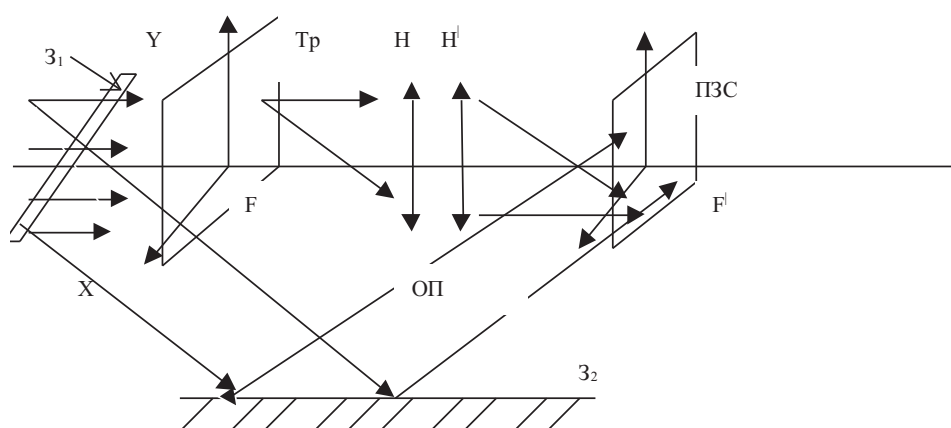


Рис. 1. Схема формирования реальной Фурье - голограммы

Тр – транспарант (слайд) с изображением, подлежащим голографированию, НН' - Фурье-объектив; F – передний фокус, в котором располагается объект; F' – задний фокус, в котором формируется Фурье-образ изображения объекта и располагается регистратор; З₁ – полупрозрачное зеркало; З₂ – глухое зеркало; ПЗС – прибор с зарядовой связью (фотоприемник), либо любой квадратичный регистратор; ОП – опорный пучок. Значение угла между объектным и опорным пучками является ключом для восстановления голограммы

Схему на рис. 1 можно интерпретировать следующим образом:

- 1) Транспаранту T_r соответствуют файлы с изображениями динамически меняющегося тест – объекта;
- 2) Объектив HN^1 моделируется преобразованием Фурье от функции, кодирующей изображения;
- 3) Взаимодействие ОП с распределением поля, моделируемым преобразованием Фурье от функции, кодирующей изображения, описывается сложением с полем комплексной амплитуды наклонной под произвольно выбранным углом плоской волны.

3.2. Синтез цифровой голограммы Фурье

Цифровые голограммы Фурье моделируют классические процессы и представляют собой запись пространственного преобразования Фурье от рассеянного виртуальным предметом светового поля со сдвинутой виртуальной пространственной несущей. В общем случае алгоритм синтеза изображения ЦВЗ для получения голограммы $h(x,y)$ выглядит следующим образом:

- 1) В виртуальной предметной области (x,y) формируется изображение ЦВЗ $W(x,y)$;
- 2) ЦВЗ переносится в плоскость пространственных частот (u,v) со смещением относительно осей координат на значения M, N : $W(u-M, v-N)$;
- 3) Создается зеркальное изображение ЦВЗ и получается сумма двух изображений: $\mathfrak{F}\{h(x,y)\} = \tilde{V} \quad W(u-M, v-N) + \gamma W(-u-M, -v-N)$, где γ – коэффициент усиления;
- 4) Для получения исходного распределения $h(x,y)$ выполняется обратное преобразование Фурье: $h(x,y) = \mathfrak{F}^{-1}\{\tilde{V}\}$, где \mathfrak{F}^{-1} – оператор обратного преобразования Фурье.

4. Описание программной реализации

Программы реализованы в среде Matlab. На рис. 2 представлен графический интерфейс системы, позволяющей пользователю сокрыть данные в изображении при помощи алгоритма на основе квантования. Для встраивания данных пользователь должен выбрать изображение, в которое они будут встраиваться.

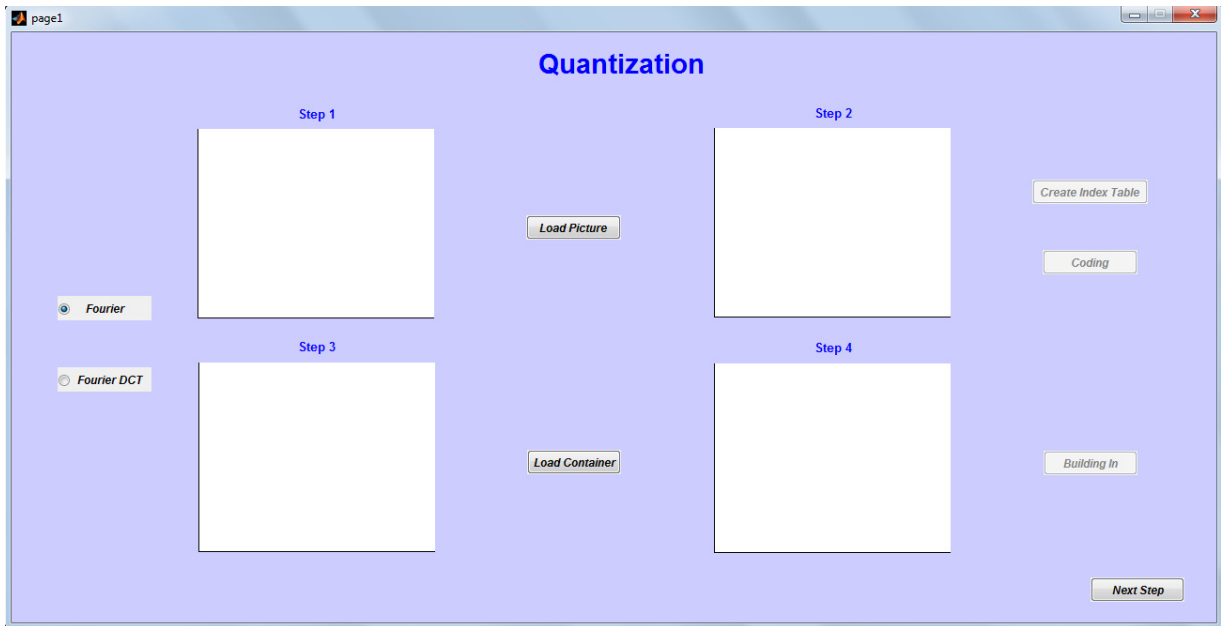


Рис. 2. а) Интерфейс программы встраивания данных

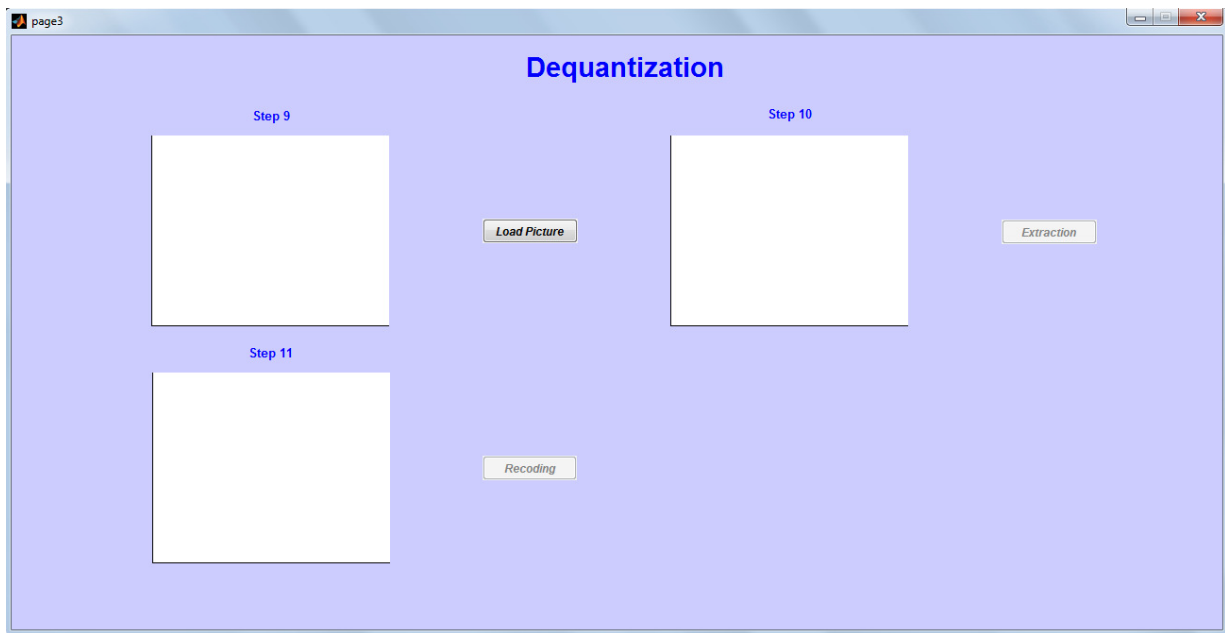


Рис. 2. б) Интерфейс программы извлечения данных

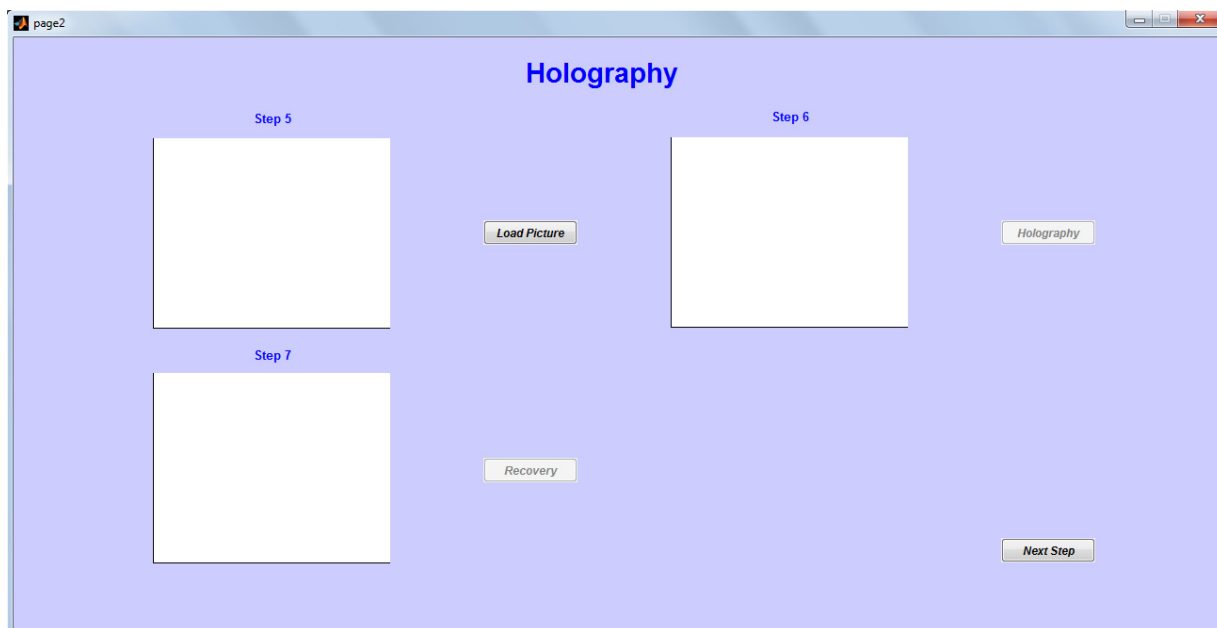


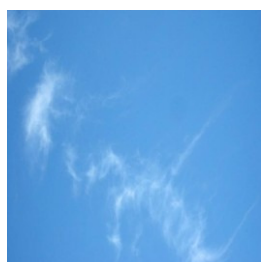
Рис. 3. Интерфейс программы получения голограммы и восстановления изображения

На рис. 3 представлен графический интерфейс программы, позволяющей пользователю преобразовывать изображение, т.е. создать голограмму Фурье.

5. Сравнение результатов



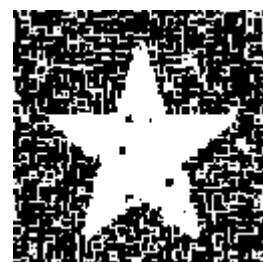
а) Встраиваемое изображение (Сообщение)



б) Контейнер



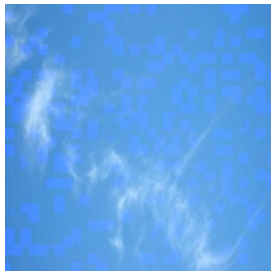
в) Контейнер со встроенным сообщением



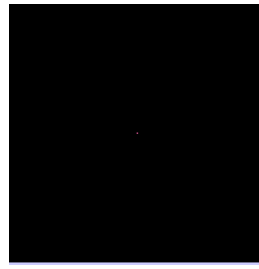
г) Извлеченное сообщение

Рис. 4. Этапы встраивания и извлечения данных, используя алгоритм на основе квантования

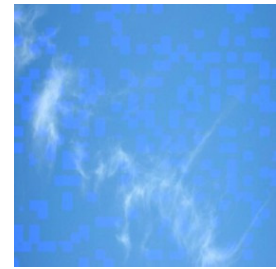
Из приведённых изображений видно, что алгоритм сокрытия данных на основе квантования даёт результат с погрешностью. Непосредственное использование этого метода в проектной документации САПР приводит к порче файлов и потере данных (изображение может быть восстановлено, но некоторые фрагменты будут искажены).



а) Исходное изображение



б) Модифицированное
изображение
(Голограмма Фурье)



в) Восстановленное
изображение

Рис. 5. Этапы создания голограммы и восстановления изображения на её основе

На рис. 5 представлены результаты работы программы реализации голограммы Фурье.

Заключение

В результате проведения данной работы были разработаны программы для преобразования и сокрытия информации на основе комбинированного метода стеганографии. Достоинством данной реализации является то, что если при передаче данных будет обнаружено наличие встроенного сообщения в изображении, понадобятся параметры, с помощью которых станет возможным восстановление изображения из голограммы. Это потребует дополнительных вычислительных и интеллектуальных ресурсов. К недостаткам можно отнести возможность удаления защищённой информации или её части из файла при передаче по сети интернет. А также непосредственное использование этого метода в проектной документации САПР приводит к порче файлов и потере данных (изображение может быть восстановлено, но некоторые фрагменты будут искажены). В рамках данного проекта поставленные задачи были выполнены.

Список литературы

1. Гонсалес Р., Вудс Р., Эддинс С. Цифровая обработка изображений в среде MatLab. М.: Техносфера, 2006. 621 с.
2. Волосатова Т.М., Денисов А.В., Чичварин Н.В. Комбинированные методы защиты данных в САПР // Информационные технологии. 2012. № 5. Приложение. С. 1-32.
3. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. М.: Салон-пресс, 2009. 272 с.
4. Poon T-Ch. Optical Scanning Holography with MATLAB. Virginia: Virginia Tech, 2007. 153 p.

5. Бадриев И.Б., Бандеров В.В., Задворнов О.А. Разработка графического пользовательского интерфейса в среде MatLab. Казань: Казанский государственный университет, 2010. 113 с.