

УДК 519.25

Разработка программной реализации комбинированного метода для сокрытия информации на основе цифровой голограммы Френеля и алгоритма LSB

Спасёнов А.Ю., студент

*Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Системы автоматизированного проектирования»*

Научный руководитель: Волосатова Т.М., к.т.н., доцент

Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана

bauman@bmstu.ru

Постановка задачи

Целью работы является разработка приложения для сокрытия информации на основе синтеза цифровой голограммы Френеля и метода LSB. В основе комбинированного метода заложено два этапа – получение цифрового голографического изображения защищаемых данных, а затем внедрение в контейнер методом LSB.

В рамках работы выполнены исследование методов стеганографии и их программная реализация. Разработано программное средство с графическим интерфейсом, позволяющее пользователю преобразовать изображение с помощью голографического метода, а также скрывать и извлекать информацию из изображений с использованием метода LSB. Получены результаты тестирования разработанного ПО, их анализ представлен в данной работе.

Метод LSB

Метод LSB (Least Significant Bit, наименьший значащий бит) — суть этого метода заключается в замене последних значащих битов в контейнере (изображения, аудио или видеозаписи) на биты скрываемого сообщения. Разница между пустым и заполненным контейнерами должна быть не ощутима для органов восприятия человека.

Младший значащий бит изображения несет в себе меньше всего информации. Известно, что человек в большинстве случаев не способен заметить изменений в этом бите. Фактически, LSB — это шум, поэтому его можно использовать для встраивания информации путем замены менее значащих битов пикселей изображения битами секретного сообщения. При этом для изображения в градациях серого (каждый пиксель

изображения кодируется одним байтом) объем встроенных данных может составлять 1/8 от общего объема контейнера.

Популярность данного метода обусловлена его простотой и тем, что он позволяет скрывать в относительно небольших файлах большие объемы информации (пропускная способность создаваемого скрытого канала связи составляет при этом от 12,5 до 30%). Метод, зачастую, работает с растровыми изображениями, представленными в формате без компрессии (например, BMP и GIF).

Метод LSB имеет низкую стеганографическую стойкость к атакам пассивного и активного нарушителей. Основной его недостаток – высокая чувствительность к малейшим искажениям контейнера.

Голограмма Френеля.

Аналоговая голография Фурье и Френеля.

Как известно, голография изначально представляла собой совокупность методов регистрации трехмерных изображений за счет кодирования координаты вдоль направления распространения электромагнитной волны в фазовой части.

Принципиальная схема голографической модели представлена на Рис. 1 и на Рис. 2.

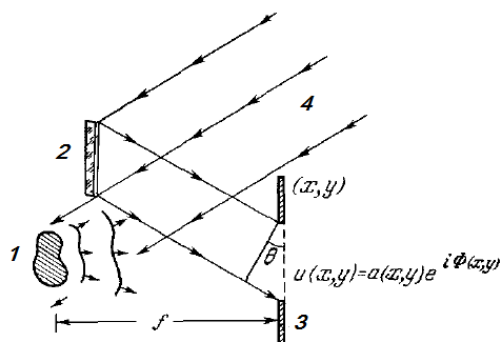


Рис. 1. Схема получения голограммы:

- 1 – предмет
- 2 - зеркало, создающее эталонный пучок
- 3 - плоскость зрчка
- 4 - когерентный источник света

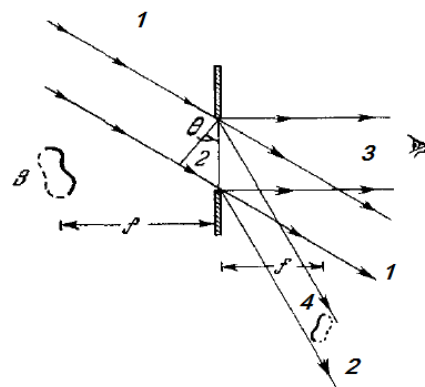


Рис. 2. Схема восстановления волны:

- 1 – эталонный пучок
- 2 - голограмма
- 3 – мнимое изображение предмета
- 4 – действительное изображение предмета

Голография, как правило, реализуется двухступенчатым процессом. На первом этапе фиксируется распределение интенсивности результата интерференции рассеянной волны от объекта и опорной волны, это и является голограммой. На втором этапе

полученную голограмму используют как дифракционный транспарант. При этом, в зависимости от задачи, восстановленное поле строит изображение объекта или некий образ, характеризующий объект.

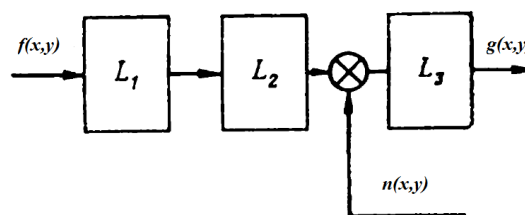


Рис. 3. Функциональная модель голографического процесса

Функциональная модель, приведенная на рисунке 3, описывает в общем виде задачу преобразования, записи голограммы и восстановления оптического изображения. Входной сигнал $f(x,y)$ распространяется от плоскости объекта до плоскости голограммы, чему соответствует система с оператором L_1 . При записи преобразованного сигнала $L_2[L_1[f(x,y)]]$ на голограмму накладываются шумы детектора $n(x,y)$. Для восстановления сигнала используют дополнительную систему L_3 .

Синтез цифровых голограмм Фурье и Френеля

Цифровые голограммы Фурье моделируют классические 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: $\mathfrak{Z}\{h(x,y)\} = \tilde{V} \quad W(u-M, v-N) + \gamma W(-u-M, -v-N)$, где γ – коэффициент усиления;

4) Для получения исходного распределения $h(x,y)$ выполняется обратное преобразование Фурье: $h(x,y) = \mathfrak{F}^{-1}\{\tilde{U}\}$, где $\mathfrak{F}^{-1}$ - оператор обратного преобразования Фурье.

При моделировании голограммы Френеля процесс создания голограммы выглядит следующим образом:

- 1) В задаче синтеза голограммы естественно считать, что объект характеризуется достаточно гладкой функцией: $u(x,y)$
- 2) Дополнительный пучок, называемый опорным пучком, должен быть направлен под углом к плоскости пластинки: u_0
- 3) Задача синтеза голограммы Френеля сводится к расчёту матрицы $\{\Gamma(r,s)\}$
- 4) Исходная функция, характеризующая объект, может быть восстановлена по её отсчётам путём интерполяции их некоторой функцией $\varphi(x,y)$

Описание программной реализации

Программы реализованы в среде Matlab. На рис. 3 представлен графический интерфейс системы, позволяющей пользователю преобразовывать изображение, т.е. создать голограмму Френеля.

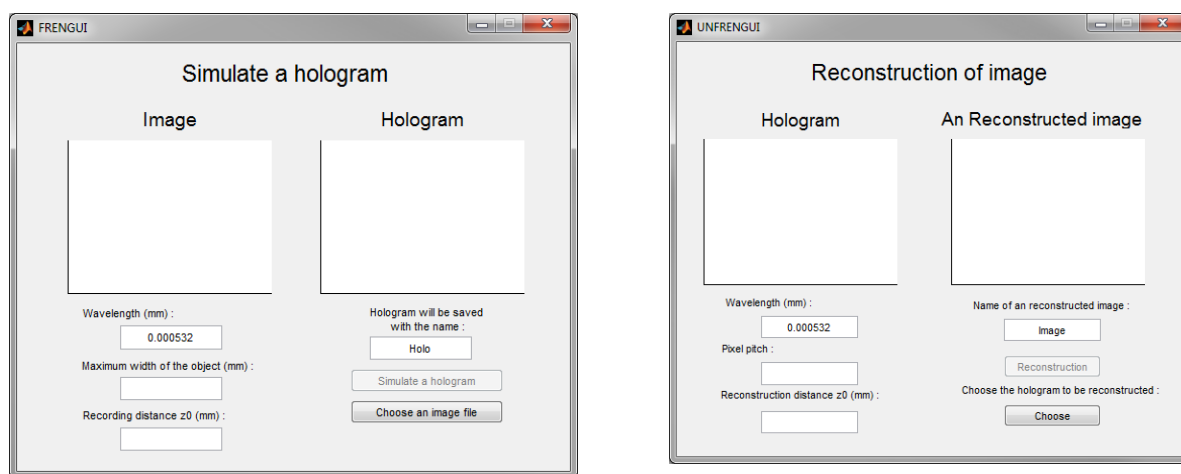


Рис. 4. Графический интерфейс программы, реализующей голограмму Френеля:

- а) Интерфейс программы создания голограммы б) Интерфейс программы восстановления изображения

С помощью данных программы пользователь может модифицировать изображение, установив необходимые параметры (ключи) для моделирования голограммы Френеля.

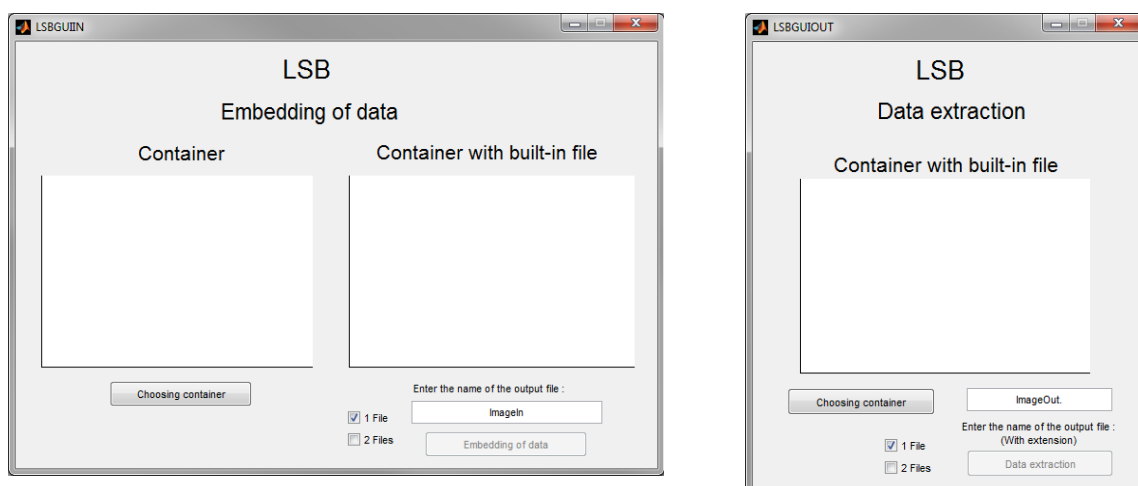


Рис. 5. Графический интерфейс программы, реализующей метод LSB:

а) Интерфейс программы встраивания данных

б) Интерфейс программы извлечения данных

На рис. 5 представлен графический интерфейс программы, позволяющей пользователю сокрыть данные в изображение. Для встраивания данных пользователь должен выбрать изображение, в которое они будут встраиваться.

Сравнение результатов

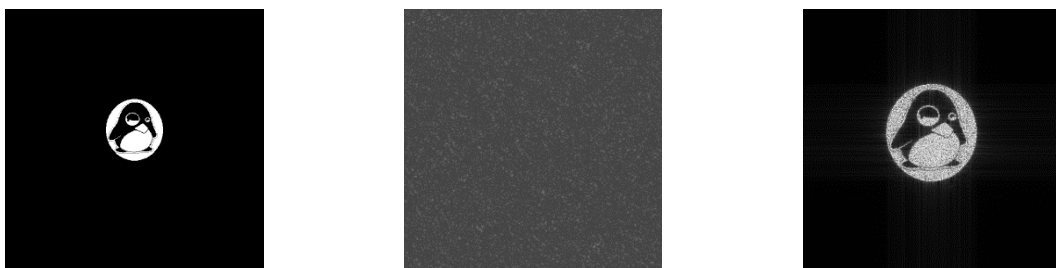


Рис. 6 – Этапы создания голограммы и восстановления изображения на её основе:

а) Исходное изображение

б) Модифицированное
изображение
(Голограмма Френеля)

в) Восстановленное
изображение

Из приведённых изображений видно, что алгоритм сокрытия данных, основанный на голограмме Френеля, даёт хороший результат. Однако, непосредственное использование этого метода в проектной документации САПР приводит к порче файлов и потере данных (изображение может быть восстановлено, но некоторые фрагменты будут искажены).



Рис. 7. Этапы встраивания и извлечения данных, используя метод LSB:

- | | | |
|---|--|-----------------------------|
| а) Встраиваемое
изображение
(Сообщение) | б) Контейнер со встроенным
сообщением | в) Извлеченное
сообщение |
|---|--|-----------------------------|

На рисунке 7 представлены результаты работы программы встраивания данных в изображение на основе метода LSB. На основе результатов можно убедиться, что при замене наименее значимых битов очень трудно заметить наличие встроенного сообщения в изображение человеческим глазом.

Заключение

В рамках данной работы было создано программное средство для преобразования и внедрения информации на основе комбинированного метода стеганографии. Преимуществом данной реализации является возможность скрытой передачи большого объема информации. Если при передаче данных будет обнаружено наличие встроенного сообщения в изображение, понадобятся параметры, с помощью которых будет возможно восстановить изображение из голограммы. Это потребует дополнительных вычислительных и интеллектуальных ресурсов. К недостаткам можно отнести возможность удаления защищенной информации или её части из файла при передаче по сети интернет.

Список литературы

1. Волосатова Т.М., Денисов А.В., Чичварин Н.В. Комбинированные методы защиты данных в САПР // Информационные технологии. 2012. С. 1-32.
2. Гонсалес Р., Вудс Р., Эддинс С. Цифровая обработка изображений в среде MATLAB. М.: Техносфера, 2006. 616 с.

3. Бадриев И. Б., Бандеров В. В., Задворнов О. А. Разработка графического пользовательского интерфейса в среде MATLAB. Казань: Изд-во Казанский государственный университет, 2010. 113 с.
4. Poon T-Ch. Optical scanning holography with MATLAB. Virginia: Virginia Tech, 2007. 153 p.
5. Кольер Р., Беркхфрт К., Лин Л. Оптическая голография. М.: Мир, 1973. 698 с.
6. Смоленцев Н. К. Создание Windows-приложений с использованием математических процедур MATLAB. М.: ДКМ, 2008. 453 с.
7. Кетков Ю., Кетков А., Шульц М. MATLAB 7 программирование, численные методы. С.-П.: БХВ-Петербург, 2005. 753 с.