УДК 003.26 004.7 004.9

СТЕГАНОГРАФИЧЕСКИЙ АЛГОРИТМ ЗАЩИТЫ ПРОЕКТНОЙ ДОКУМЕНТАЦИИ

Медведев Н.В., Чичварин Н.В.
МГТУ им. Н.Э. Баумана
Москва, Российская Федерация

Введение. Задача защиты проектной документации от несанкционированного доступа остается весьма актуальной. Как показывает обзор публикаций [1-7], в настоящее время нет известных удовлетворительных решений в области решения задачи защиты проектной документации, продуцируемых в среде САПР. Достаточно убедительно актуальность проблемы подчеркивают Указ Президента России «О концепции национальной безопасности РФ» от 10.01.2000 г.

Современные САПР опираются на применение PLM – технологий, в часности CALS. Как известно, такие системы предполагают необходимость передачи проектной документации по окрытым каналам. Авторами предложен метод сокрытия данных, который представляется приемлемым для решения поставленной задачи.

Цель исследований. Целью исследований, результаты которых изложены в настоящей публикации явился сопоставительный анализ алгоритмов стегнографического шифрования проектной документации в САПР, опирающихся на CALS – технологии. В качестве критериев установлены:

- Скрытность проектных, передаваемых по открытым каналам.
- Устойчивость к атакам.
- Скорость передачи даннных.

В процессе проведенных исследований рассмотрены комбинированные методы стеганографии:

- Метод, использующий цифровую Фурье-голографию.
- Метод, использующий вычисление функции взаимной корелляции.

Описание результатов анализа. Первый алгоритм реализуется двумя основными этапами:

- Определяется цифровая Фурье-голограмма проектной изображения проектной документации.
- Полученное изображение заносится в контейнер одним из известных алгоритмов.

Дешифровка осуществляется в обратном порядке:

- Голограмма извлекается из контиейнера с помощью известного ключа.
- Изображение документации получается восстановлением голограммы.

Рассмотрим результаты численного эксперимента, проведенного с применением программы, реализующей алгоритм формирования и восстановления цифровой Фурье-голограммы.

На рисунке 1 приведено изображение маскируемой документации.

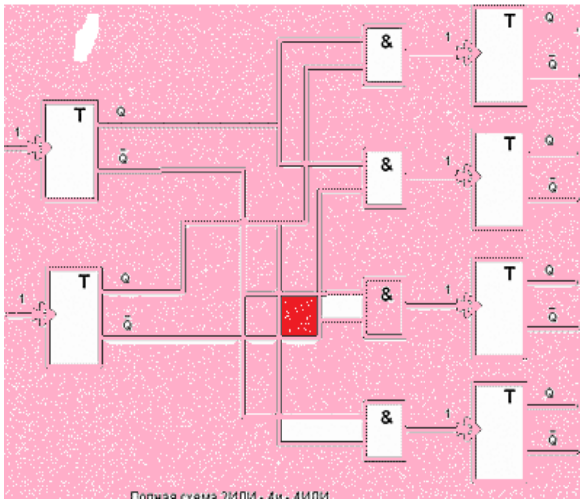

Рисунок 1 – Схема голографируемой документеции

На рисунке 2 приведено изображение соответствующей голограммы.

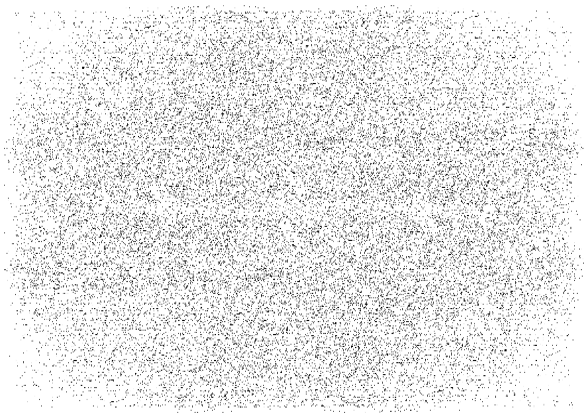

Рисунок 2 – Изображение Фурье-голограммы изображения, приведенного на рисунке 1

Этапы алгоритма следующие:

- Вычисление корелляционной функции, моделирующей распределение контраста в изображении шифруемой схемы функции, с функцией, моделирующей распределение контраста в изображении кодирующей схемы («слепой»

схемы). Авторы предложили применять вычисление свертки при вычислении корелляционной функции, поскольку в данном случае изображения кодируются вещественными функцями.

- Внедрение результата первого этапа в контейнер любым из известных методов стеганогрфии.

Так же, как и в первом алгоритме, восстановление изображения зашифрованной окументации ощуществляется в порядке, обратным процессу шифровки.

Рассмотрим упрощенную модель системы дефокусировки, описываемую интегральным уравнением Фредгольма первого рода [8-10]:

$$\int_a^b k(p,x,s_x,y,s_y)g(s_x,s_y)ds_x ds_y = f(x,y),$$

где: s_y – пространственные координаты, $k(\mathbf{p},x,s_x,y,s_y)$ – ядро интегрального уравнения, описывающее виртуальную систему дефокусировки.

p – векторный параметр, задаваемый в случае, если уравнение описывает пространственно неинвариантную систему, т.е когда импульсный отклик параметрически зависит от положения в поле зрения оптической системы. Это характерно для нереально широкополосных систем. Оно же является импульсным откликом линейной си-стемы и преобразование Фурье от него, как известно, является передаточной функцией. Параметры «импульсного отклика» виртуальной системы являются дополнительным ключом.

g(. , .) – распределение интенсивности в кодирующем изображении - финитная функция,

f(. , .) – распределение интенсивности в защищаемом изображении – финитная функция,

<a , b> – область финитности.

Уравнение записано в самом общем виде, т.е. учитывает пространственную инвариантность виртуальной дефокусирующей системы.

Для большинства реальных систем и, особенно в случае моделирования дефокусировки на ЭВМ это алгоритм решения этого уравнения имеет большую вычислительную сложность.

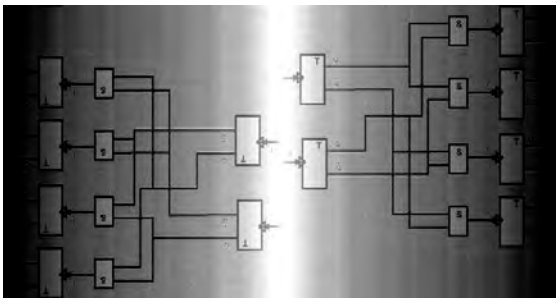

Рисунок 3 – Восстановленная голограмма

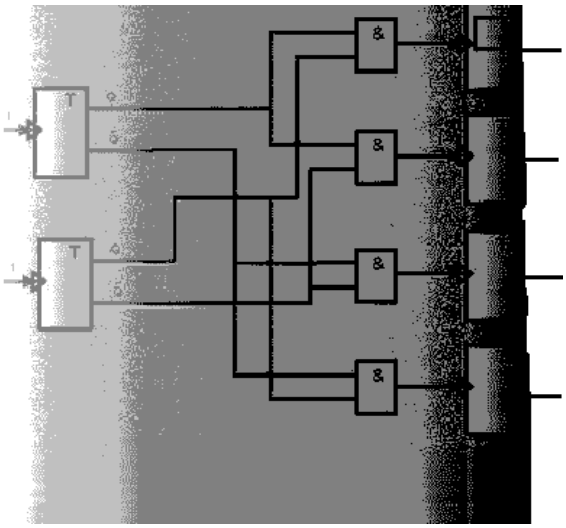

Рисунок 4 – Неполное препарированное восстановленное изображение голограммы

Для упрощения задачи предлагается применить простой и удобный метод слепой деконволюции. Метод основан на решении обратной задачи. Особенностью предъявляемого алгоритма является:

Решение задачи конволюции на основе вычисления ковариационной функции:

$$Cov(v,u) = \iint_{-\infty}^{\infty} f1(x,y)f2(x-v,y-u)\,dx\,dy,$$

где $Cov(v,u)$ – ковариационная функция,

f1(x,y) – функция, моделирующая распределение контраста в исходном изображении,

f2(x,y) – функция, моделирующая распределение контраста в кодирующем изображении.

Так как *f(x,y)* является вещественной, автосовариации может быть реализована, как свертка, для ускорения возможно вычисление в спектраль-ной области:

$$Cov(v,u) = F^{-1}(F\big(f(v,u)F(v,u)\big),$$

где $Cov(v,u)$ – ковариационная функция,

$F^{-1}\{*\}$ – оператор обратного преобразования Фурье,

$F\{*\}$ – оператор прямого преобразования Фурье.

Восстановление изображения осуществляется с помощью решения задачи деконволюции. Наиболее простой и достаточно точным является метод слепой деконволюции:

$$F^{-1}\{G(v,u)\} = F\{Cov(x,y)\}/[F\{(f(x,y)\} + a]$$

Где *Cov(x,y)* – ковариационная функция,

a – регуляризирующиий параметр, который подбирается «вслепую», т.е. по субъективному восприятию.

Примеры решения задачи вычисления ковариационной функции и результат деконволюции приведены на Рисунках 5-8.

Как видно, результаты вполне удовлетворительны. Можно считать, что предложенный алгоритм достаточно устойчив к атакам, так как для распознавания стего необходимо во – первых, установить метод сокрытия, а затем – определив, что нужно восстанавливать исходное по известному заранее кодирующему изображение «слепой» документации, которое не содержит ничего полезного для злоумышленника.

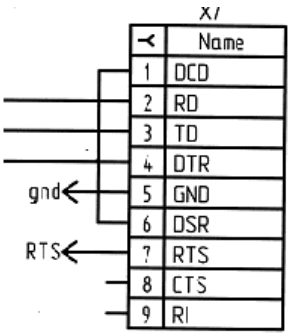

Рисунок 5 – Исходное (шифруемое) изображение

Рисунок 6 – Зашифрованное изображение

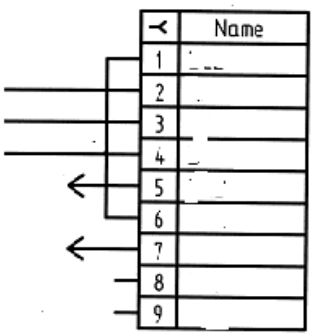

Рисунок 7 – Кодирующее изображение («слепая» распиновка)

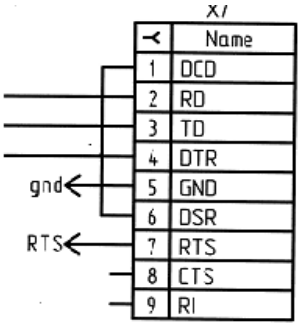

Рисунок 8 – Восстановленное изображение

Заключение. Проведенные исследования и полученные результаты, часть которых приведена в работе, позволяют сделать следующие выводы:

1. Проведен анализ известных стеганографических алгоритмов.
2. Предложены оригинальные двухступенчатые метод сокрытия данных, в частности проектной документации, разрабатываемой в частности, в САПР.
3. Проведены экспериментальные исследования, результаты которых подтвердили преимущества предложенных алгоритмов.
4. Предложенный комбинированный алгоритм применим в технологиях PLM.

1. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая Стеганография. М.: СОЛОН-Пресс. – 2002. – 272с.
2. Rotation scale and translation invariant spread spectrum digital image watermarking. IEEE Int. Conf. on Image Processing. – 1998. – P. 4.
3. Pereira S., Joseph J., Deguillaume F. Template Based recovery of Fourier-Based Watermarks Using log-polar and Log-log Maps. IEEE Int. Conf on Multimedia Computing and Systems. – 1999. – P. 5.
4. Lin Ch-Y., Chang Sh.-F. Distortion Modeling and Invariant Extraction for Digital Image Print- and Scan Process. International Symposium on Multimedia Information Processing. – 1999. – P. 10.
5. Lin Ch-Y., Chang Sh.-F. Public Watermarking Surviving General Scaling and Cropping: An Application for Print-and-Scan Process. Multimedia and Security Workshop at ACM Multimedia. – 1999.
6. Pereira S., Thierry P. Fine Robust Template Matching for Affine Resistant Image Watermarks. IEEE Trans. on Image Processing. – 1999. – P. 12.
7. Wiener N. Extrapolation, Interpolation, and Smoothing of Stationary Time Series. – New York : Wiley. – 1949.