УДК 621.391

Б.Ф. БАДАЛЯН, И.А. ПОГОСЯН

ПРОГРАММНАЯ РЕАЛИЗАЦИЯ СТЕГАНОГРАФИЧЕСКОЙ СИСТЕМЫ ВСТРАИВАНИЯ ИНФОРМАЦИИ

Рассматриваются основные принципы стеганографического встраивания конфиденциальной информации. Представлены методы встраивания информации в пространственную и частотную области цифровых изображений на основе дискретного вейвлет-преобразования и алгоритма LSB. Разработана программная реализация стегосистемы сокрытия текстовой информации в среде MATLAB R2021a, криптостойкость которой обеспечивается применением асимметричного алгоритма RSA.

Ключевые слова: конфиденциальность, стеганография, стегосистема, контейнер, цифровые водяные знаки, робастность, вейвлет-преобразование, алгоритм RSA.

Введение. Широкое распространение мультимедийных технологий, сети Интернет, непрерывное совершенствование компьютерной техники, методов цифровой обработки информации определило развитие стеганографии, которая, в отличие от криптографии, не маскирует содержимое секретного сообщения, а скрывает сам факт его существования или передачи. Стеганографию обычно используют совместно с методами криптографии, таким образом, дополняя и усиливая её.

Общей особенностью всех стеганографических методов является то, что скрываемое сообщение внедряется в некоторый, не привлекающий внимания нейтральный объект (цифровой контейнер). При применении криптографических преобразований наличие зашифрованного сообщения само по себе привлекает внимание, в то время как стеганография обеспечивает незаметность существования конфиденциальной информации.

Основной принцип работы стеганографической системы приведен на рис.1. Контейнер в подобной системе является носителем сокрытой информации, а стегоключ определяет конкретный вид алгоритма сокрытия информации. Следует отличать стеганографический ключ от криптографического, который также может присутствовать в системе и использоваться для предварительного криптографического закрытия внедряемой информации.

По аналогии с криптографией, по типу стегоключа стеганографические системы можно подразделить на три типа: с секретным ключом, с открытым ключом и гибридные.

Алгоритм стеганографического встраивания информации в общем случае должен обеспечивать невозможность обнаружения сокрытой информации несанкционированным получателем. Дополнительным требованием является робастность – устойчивость стегоконтейнера к различным воздействиям, возникающим при его обработке и передаче по каналам связи.

Рис. 1. Структура стеганографической системы

В последнее время для подтверждения подлинности передаваемых данных, предотвращения несанкционированного доступа к ним и защиты контейнера широко применяются также системы встраивания цифровых водяных знаков (ЦВЗ). Выделяют три класса методов встраивания ЦВЗ: хрупкие, полухрупкие и робастные. Хрупкий ЦВЗ разрушается от любого воздействия на контейнер, полухрупкий ЦВЗ устойчив к некоторым преобразованиям, робастный ЦВЗ обнаруживается в цифровом объекте даже после существенных искажений [1].

Основная часть. Наиболее популярными контейнерами для встраивания являются цифровые изображения. Все методы стеганографического сокрытия информации в цифровых изображениях делятся на методы сокрытия в пространственной области и методы сокрытия в частотной области [2]. Сокрытие в пространственной области предполагает изменение пикселей изображения, сокрытие в частотной области – изменение частотных коэффициентов, полученных после применения к пикселям некоторого частотного преобразования.

Простейшим методом встраивания скрытой информации является LSB (Least Significant Bit, Наименьший Значащий Бит), когда секретная информация встраивается в младшие значащие биты контейнера-медиафайла. Изменение последнего бита значения пикселя не приводит к визуально заметному

изменению изображения, а это означает, что перехватчик не сможет отличить исходное изображение от стеганографически модифицированного.

Метод LSB достаточно прост в реализации, одновременно обеспечивается высокая полезная емкость контейнера. Однако встроенная информация является хрупкой, так как при любом искажении контейнера она искажается [3]. Для определения полезной емкости контейнера при использовании метода LSB необходимо воспользоваться формулой

$$Q = H \cdot W \cdot V \cdot D, \tag{1}$$

где Q - емкость контейнера в битах; H- высота изображения в пикселях; W - ширина изображения в пикселях; V - число цветовых компонент; D- количество наименее значащих битов в каждой компоненте.

Как известно, набор вейвлетов в их временном или частотном представлении может приближать сложный сигнал или изображение, причем как идеально точно, так и с некоторой погрешностью. Прямое непрерывное вейвлет-преобразование сигнала $s(t)$ реализуется по формуле

$$C(a,b) = \int_{-\infty}^{\infty} s(t) a^{-1/2} \psi\left(\frac{t-b}{a}\right) dt, \tag{2}$$

где параметр b задает положение вейвлетов, а параметр a - их масштаб.

Непрерывное вейвлет-преобразование не может применяться в стеганографии для минимизации вносимых искажений и устойчивости к атакам пассивного злоумышленника, так как требует больших вычислительных затрат при его проведении. Для практического применения необходима дискретизация значений параметров a и b.

При дискретных значениях a и b вейвлет-функция может быть представлена в виде [4]

$$\psi_{j,k}(t) = a_0^{-\frac{j}{2}} \psi\left(a_0^{-j} t - k\right), \tag{3}$$

где j - параметр масштаба.

Таким образом, при подстановке в формулу (1) дискретных значений a и b получаем формулу для дискретного вейвлет-преобразования:

$$C(j,k) = d_{j,k} = \int_{-\infty}^{\infty} a_0^{-\frac{j}{2}} \psi\left(a_0^{-j} t - k\right) s(t) dt, \tag{4}$$

где $d_{j,k}$ - детализирующие коэффициенты для вейвлет-декомпозиции сигнала уровня k.

Частотная область вейвлетов может быть разбита на низкочастотную и высокочастотную составляющие, частота раздела которых равна половине частоты дискретизации сигнала. Для их разделения достаточно использовать два фильтра - низкочастотный Lo и высокочастотный Hi, к входам которых подключается сигнал s. Фильтр Lo дает частотный образ для аппроксимации (грубого приближения) сигнала, а фильтр Hi - для его детализации.

Полученные фильтры передают только половину всех частотных компонент сигнала, и не попавшие в полосу прозрачности компоненты могут быть удалены [5]. Данная операция называется децимацией вдвое и обозначается как $\downarrow 2$. Если просто сложить полученные на выходах фильтров сигналы, то получится исходный сигнал, то есть будет иметь место полная реконструкция сигнала на начальном уровне. Однако Lo-фильтр можно, в свою очередь, разложить на два фильтра и подвергнуть спектры этих новых фильтров операции децимации. Таким образом, может быть сформирована система вейвлет-фильтров, реализующих операцию декомпозиции сигнала того или иного уровня.

На основе вышеизложенного в среде MATLAB R2021a была разработана стегосистема, реализующая встраивание информации в субполосы коэффициентов декомпозиции. В качестве базисного вейвлета для декомпозиции использовались вейвлеты Добеши 5-го порядка. На рис.2 представлено окно программной реализации указанной стегосистемы в режиме встраивания/извлечения конфиденциальной информации. Как видно из рисунка, после выбора контейнера активируется поле ввода секретного сообщения "Enter text message". В режиме извлечения информации выбирается заполненный стегоконтейнер, и нажатием клавиши "Decode" в текстовом поле "Decrypted text message" отображается секретное сообщение.

Для обеспечения высокой криптостойкости стегосистемы применяется асимметричная криптосистема RSA, безопасность которой основана на сложности разложения на множители больших чисел. Таким образом, восстановление скрываемого сообщения требует наличия стегоконтейнера и закрытого ключа алгоритма RSA.

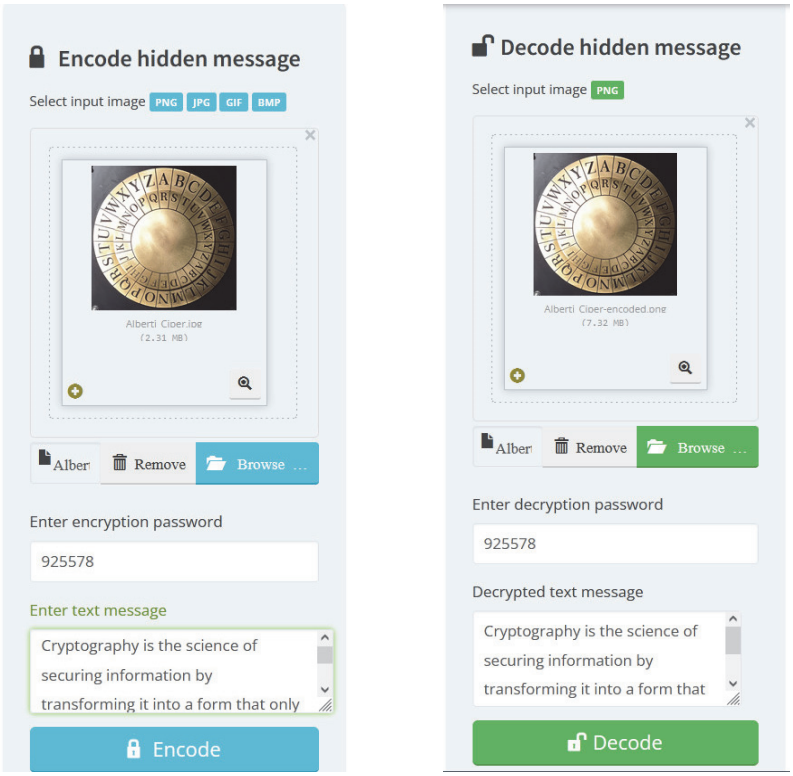

Рис. 2. Реализация стегосистемы встраивания информации

Заключение. Каждый стеганографический метод обладает как сильными, так и слабыми сторонами. Пользователю важно выбрать метод, который в наибольшей степени соответствует поставленной задаче. Существует несколько критериев для сравнения и выбора наиболее подходящей стегосистемы. Среди основных критериев сравнения можно выделить незаметность, вместимость и робастность. Методы LSB являются неустойчивыми ко всем видам атак и могут быть использованы только при отсутствии шума в канале передачи данных. Другие методы сокрытия информации в графических файлах ориентированы на форматы файлов с потерей, к примеру, JPEG. В отличие от LSB, они более устойчивы к геометрическим преобразованиям. Проанализировав полученные результаты, можно сделать вывод, что применение дискретного вейвлет-преобразования более надежно, так как позволяет скрыть сообщение в частотной области изображения-контейнера.

СПИСОК ЛИТЕРАТУРЫ

1. **Грибунин В.Г., Оков И.Н., Туринцев И.В.** Цифровая стеганография. – М.: Солон-Пресс, 2009. – 272 с.
2. **Федосеев В.А.** Цифровые водяные знаки и стеганография: Учебное пособие. — 2-е изд., исправ. и доп. — Самара: СамГУ, 2019. — 144 с.
3. **Шелухин О.И., Канаев С.Д.** Стеганография. Алгоритмы и программная реализация.– М.: Горячая линия –Телеком, 2018. – 592 с.
4. **Смоленцев Н.К.** Основы теории вейвлетов. Вейвлеты в MATLAB.- М.: ДМК Пресс, 2005.-304 с.
5. **Дьяконов В.П.** Вейвлеты**.** От теории к практике. – М.: СОЛОН-Р, 2002. – 446 с.

Բ.Ֆ. ԲԱԴԱԼՅԱՆ, Ի.Ա. ՊՈՂՈՍՅԱՆ

ԻՆՖՈՐՄԱՑԻԱՅԻ ՆԵՐԴՐՄԱՆ ՍՏԵԳԱՆԱԳՐԱՖԻԿԱԿԱՆ ՀԱՄԱԿԱՐԳԻ ԾՐԱԳՐԱՅԻՆ ԻՐԱԿԱՆԱՑՈՒՄԸ

Դիտարկված են գաղտնի ինֆորմացիայի ստեգանագրաֆիկական ներդրման հիմնական սկզբունքները: Ներկայացված են թվային պատկերների հաճախային և տարածական տիրույթներում ինֆորմացիայի ներդրման մեթոդները դիկսրետ վեյվլետ-ձևափոխության և LSB ալգորիթմի հիման վրա: MATLAB 2021a միջավայրում մշակվել է տեքստային ինֆորմացիայի քողարկման ստեգահամակարգի ծրագրային իրականացումը, որի կրիպտակայունությունն ապահովվում է RSA ասիմետրիկ ալգորիթմի կիրառմամբ:

Առանցքային բառեր. գաղտնիության, ստեգանագրաֆիա, ստեգահամակարգ, կոնտեյներ, թվային ջրանիշներ, ռոբաստություն, վեյվլետ-ձևափոխություն, RSA ալգորիթմ:

B.F. BADALYAN, I.A. POGHOSYAN

SOFTWARE IMPLEMENTATION OF A STEGANOGRAPHIC SYSTEM FOR INFORMATION HIDING

The basic principles of steganographic hiding of confidential information are considered. Methods for hiding information in the spatial and frequency domains of digital images based on the discrete wavelet transform and the LSB algorithm are presented. A software implementation of a stegosystem for hiding the text information in the MATLAB R2021a environment has been developed, the cryptographic stability of which is ensured by the use of the asymmetric RSA algorithm.

Keywords: confidentiality, steganography, stegosystem, container, digital watermarks, robustness, wavelet transform, RSA algorithm.