Для поиска уязвимостей созданы общедоступные базы данных уязвимостей, содержащие информацию о уязвимостях различного программного обеспечения [4, 5].

Одним из критериев описания уязвимостей является вид программного обеспечения, к которому относятся прикладное программное обеспечение, системное программное обеспечение, микропрограммное обеспечение, а также сетевое программное обеспечение [6].

Нарушитель, обладающий сведениями о наличии в информационной системе уязвимостей программного обеспечения, реализует угрозу безопасности информации на одном уровне информационной системы (сетевом, прикладном, системном или аппаратном). Обладая информацией о уязвимостях информационной системы на каждом и ее уровне возможности спрогнозировать действия нарушителей.

Такой подход к процессу моделирования угроз позволяет выявить угрозы безопасности информации с учетом особенности их реализации на каждом из уровней информационной системы. За счет представления информационной системы в виде уровней и прогнозирования действий нарушителей на каждом из уровней снижается количество учтенных при моделировании угроз безопасности информации.

Представленный подход к классификации угроз безопасности информации и применению данной классификации при моделировании угроз в информационных системах позволит повысить эффективность защиты информации в информационных системах.

1. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения.
2. ГОСТ Р ИСО/МЭК 27001-2013. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.
3. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.
4. Банк данных угроз безопасности информации [Электронный ресурс]. – Режим доступа: <https://bdu.fstec.ru>
5. База данных общеизвестных уязвимостей информационной безопасности [Электронный ресурс]. – Режим доступа: <https://cve.mitre.org/>
6. Общая система оценки уязвимостей [Электронный ресурс]. – Режим доступа: <https://www.first.org/cvss>

Кустов В.Н., Процко Д.К.

Использование дискретного вейвлет-преобразования для внедрения информации в изображения

*Петербургский государственный университет путей сообщения
Императора Александра I
(Россия, Санкт-Петербург)*

doi:10.18411/spc-12-06-2018-05

idsp: 000001:spc-12-06-2018-05

Abstract

Steganography is a term used for covered writing. Steganography can be applied on different file formats, such as image, audio, video, text etc. At the destination, the data is extracted from the cover image using the inverse transformation. This paper presents a new approach for image steganography using DWT. The cover image is divided into higher and lower frequency sub-bands and data is embedded into higher frequency sub-bands. Arnold Transformation is used to increase the security. The proposed approach results in high capacity image steganography as compared to existing approaches.

Keywords: steganography, stegocontainer, stegosystem, stegoanalysis, discrete wavelet transform.

Введение

Стеганография – наука о создании (внедрении) скрытых сообщений таким образом, что никто, кроме отправителя и предполагаемого получателя, не подозревает о существовании сообщения. В цифровой стеганографии электронная связь может включать в себя стеганографическое кодирование внутри объектов транспортного уровня, такое как файл документа, изображения, программа или протокол. Медиа-файлы идеально подходят для стеганографической передачи из-за их большого размера и большой избыточности. В качестве простого примера отправитель может начать с безобидного файла изображения и настроить цвет каждого сотого пикселя в соответствии с буквой в алфавите, что настолько тонко, что кто-то, кто не ищет его, вряд ли заметит его.

Методы стеганографии изображений можно разделить на две группы: те, которые находятся в пространственной области изображения, и те, которые в частотной. Методы, которые редактируют пространственную область, непосредственно влияют на сам контейнер (к примеру, изменяют пиксели изображения). Но такие методы сильно чувствительны к различным изменениям контейнера. Изменение масштаба, вращение, обрезка, добавление шума или помех в канал или различное сжатие с потерями, скорее всего уничтожит скрытое сообщение.

Методы, которые позволяют встраивать сообщения в частотную область, сначала преобразуют файл-контейнер, а затем только производят встраивание. Эти методы не зависят от форматов изображений [3], [4]. Информация, скрывающая методы стеганографии, основана на следующих преобразованиях, таких как

- Дискретное преобразование Адамара (DHT)
- Дискретное преобразование Фурье (DFT)
- Дискретное косинусное преобразование (DCT).
- Дискретное вейвлет-преобразование (DWT).
- Сингулярное разложение (SVD)

Данная статья описывает метод сокрытия данных в изображениях, основанный на дискретном вейвлет-преобразовании.

Модель стегосистемы

Существуют четыре основных требования к любому алгоритму встраивания информации:

1. Незаметность;
2. Емкость;
3. Безопасность;
4. Робастность.

Незаметность означает, что визуально невозможно определить наличие скрытого сообщения. Емкость определяет какое максимальное количество информации можно скрыть в сообщении. Безопасность означает возможность противостоять атакам, направленным на выявление или повреждение скрытого сообщения. Робастность алгоритма показывает устойчивость к различным повреждениям контейнера, к примеру, наличие помех в канале передачи или сжатию с потерями.

Отправитель, желающий послать секретное сообщение, случайным образом выбирает изображение, в которое будет встраивать информацию. Далее, отправитель встраивает сообщение в выбранное изображение и зашифровывает его так называемым стегоключом. Без этого ключа получатель и злоумышленник не может извлечь секретное сообщение. После этого отправитель передает изображение получателю по каналу связи. Получатель способен извлечь сообщение, так как он знает метод внедрения и стегоключ. Цель стегосистемы состоит в том, чтобы помешать третьей стороне обнаружить скрытое сообщение. Нарис. 1 показан общий принцип ее работы.

Дискретное вейвлет-преобразование

Вейвлет-преобразование изображения – это процесс разложения спектра изображения на набор базисных вейвлет-функций. Дискретное вейвлет-преобразование обладает отличной способностью локализации пространственных частот. ДВП разделяет сигнал (изображение) на высокочастотные и низкочастотные части [1]. Высокочастотная часть содержит информацию об основных компонентах сигнала, в то время как низкочастотная снова разделяется на высокочастотную и низкочастотную.

Рисунок 1. Модель стегосистемы

Для каждого уровня разложения сначала выполняется ДВП в вертикальном направлении, а затем ДВП в горизонтальном направлении. После каждого уровня у нас получается блок 4x4, приведенный на рис. 2.

Рисунок 2. Первый этап ДВП

Рисунок 3. Второй этап ДВП

Следующий уровень разложения выполняется в низкочастотной части, полученной в предыдущем разложении (рис. 3).

Реализация метода, основанного на использовании ДВП

Основными вещественными показателями методов сокрытия информации в стеганографии являются:

1. PSNR – пиковое соотношение сигнала к шуму;
2. Емкость;
3. Корреляция.

PSNR обратно пропорционально емкости и прямо пропорционально корреляции и наоборот. Во время исследования было выявлено правильное соотношение PSNR к емкости и корреляции, которое позволяет утверждать, что информацию можно пересылать по незащищенному каналу передачи информации, не опасаясь несанкционированного доступа третьей стороны. Но также нужно учитывать, что чем больше закладка, тем сильнее ее воздействие на стегоконтейнер и для больших данных необходимо выбирать контейнер большего размера.

Отображение «кота Арнольда»

В математике, отображение «кота Арнольда» – хаотичное отображение на торе, названное в честь кота Владимира Арнольда [2].

$$\Gamma\left(\begin{bmatrix} x \\ y \end{bmatrix}\right) = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod 1 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod 1.$$

Рисунок 4. Алгоритм встраивания закладки

Алгоритм встраивания закладки

В предлагаемом подходе ДВП используется для разложения изображения высокочастотные и низкочастотные поддиапазоны. Секретные данные преобразуются с использованием отображения «кота Арнольда». В данном алгоритме секретное изображение разделяется на компоненты RGB и внедряется в поддиапазон HL. После внедрения применяется обратное ДВП, компоненты собираются обратно и получается заполненный стегоконтейнер. Предложенный алгоритм представлен на рис 4.

Статистический анализ

Пиковое соотношение сигнала к шуму (PSNR) – означает соотношение между максимумом возможного значения сигнала и мощностью шума, искажающего значения сигнала [5]. Эта метрика используется для отображения разницы пустого и заполненного контейнеров:

$$PSNR = 10 \lg \left(\frac{255^2}{MSE} \right).$$

Среднеквадратичная ошибка (MSE) – определяет разницу между интенсивностями заполненного и пустого контейнеров:

$$MSE = \frac{1}{M \times N} \sum_{i=1}^M \sum_{j=1}^N (f(i, j) - f'(i, j))^2.$$

Где - $f(i, j)$ – пустой контейнер, а $f'(i, j)$ – заполненный контейнер. Большое значение MSE обозначает, что исходное изображение плохого качества, и наоборот.

Емкость – процентное соотношение размеров исходного изображения и закладки. Она рассчитывается по формуле:

$$Capacity = \frac{\text{Кол} - \text{во пикселей секретного сообщения}}{\text{Кол} - \text{во пикселей, используемых для скрытия данных}}.$$

Корреляция – используется для отображения линейной зависимости между двумя контейнерами [6]:

$$r_{xy} = \frac{\sum_{i=1}^n (x_i - \bar{x})(y_i - \bar{y})}{(n - 1)s_x s_y}.$$

Результаты испытаний

В таблице 1 показаны основные показатели работы данного алгоритма. Как видно из таблицы, предложенный метод отлично справляется с сокрытием данных в изображении.

N	Размеры контейнера	Размер закладки	PSNR пустого контейнера	PSNR заполненного контейнера	Корреляция	Емкость
1	1680 x 1050	635 x 715	45.0553	15.2341	0.9997	0.29
2	1440 x 990	635 x 715	47.8423	20.4323	0.9998	0.26
3	1360 x 768	600 x 400	49.3421	12.2342	0.9997	0.22

Заключение

В представленной статье рассматривается алгоритм сокрытия данных с использованием дискретного вейвлет-преобразования, преобразования Арнольда и обратного дискретного вейвлет-преобразования. Преобразование Арнольда в данной комбинации используется для повышения безопасности. Оно позволяет извлечь полноценную закладку только получателю, владеющему информацией о способе встраивания. Предлагаемый метод является попыткой устранить недостатки предыдущих аналогичных стеганографических методов. Результат работы метода приведен в виде извлеченного изображения. Результаты PSNR, емкость и корреляция показаны в таблице. Из приведенных показателей можно сделать вывод о том, что

предлагаемый метод обладает хорошим показателем PSNR, а значит обладает и высокой способностью встраивания.

1. Amitava Nag, Sushanta Biswas, Debasree Sarkar and Partha Pratim Sarkar, "A Novel Technique for Image Steganography Based on DWT and Huffman Encoding", International Journal of Computer Science and Security, (IJCSS), Vol. 4, No. 6, pp 561- 570, 2010 [15].
2. Divya Saxena, "Digital Watermarking Algorithm based on Singular Value Decomposition and Arnold Transform", International Journal of Electronics and Computer Science Engineering (IJECSSE)", Vol. 1, No. 1, pp 22-27
3. David Frith, "Steganography Approaches, Options and Implications", Network Security, August 2007.
4. Abbas Cheddad, Joan Condell, Kevin Curran and Paul McKeivitt, "Biometric Inspired Digital Image Steganography", IEEE.
5. R. Amirtharajan, R. Akila, P. Deepika Chowdavarapu, "Comparative Analysis of Image Steganography", International Journal of Computer Applications, volume 2 – No.3, May 2010.
6. S.K. Muttou, Sushil Kumar, "A multilayered secure, robust and high capacity image steganographic algorithm", 2011.

Литвиненко Р.С.

Исследование прототипа микромодуля хранения информации с повышенной устойчивостью к радиационному излучению

*Научно-производственный комплекс «Технологический центр»
(Россия, Москва, Зеленоград)*

doi:10.18411/spc-12-06-2018-06

ids: 000001:spc-12-06-2018-06

На сегодняшний день одно из наиболее быстро развивающихся направлений в микроэлектронике – это создание радиационно-стойкой электронной компонентной базы для аппаратуры с повышенной устойчивостью к воздействиям ионизирующего излучения космического пространства. Движущей силой в данном случае является растущий рынок запусков космических аппаратов и транспортных систем различного назначения. Воздействие ионизирующего излучения космического пространства предъявляет повышенные требования к микросхемам по устойчивости к сбоям. Особенно остро стоит вопрос сохранности информации на запоминающих устройствах в условиях повышенной радиации.

Объектом исследования является прототип микромодуля оперативного хранения информации бортовой аппаратуры космических аппаратов. Прототип микромодуля имеет в составе программируемую логическую интегральную схему (ПЛИС), на которой реализован контроллер управления, флэш-память, а также микросхему тиристорной защиты. Электрическая схема микромодуля представлена на рисунке 1.

Контроллер управления выполняет задачи доступа, чтения, записи информации в микросхему памяти. Задача контроллера управления также состоит в повышении радиационной стойкости микромодуля за счет применения корректирующих кодов. Контроллер может быть реализован на основе базового матричного кристалла (БМК) или программируемой интегральной схемы (ПЛИС).

В НПК «Технологический центр» разработан БМК серии 5503, который может быть использован для разработки контроллера управления микромодуля.

Серия БМК 5529 является более продвинутой разработкой по сравнению с серией 5503 и является предпочтительным вариантом к моменту изготовления конечных изделий. Технология изготовления позволяет существенно снизить время задержки сигналов и повысить быстродействие.

Однако вариант реализации контроллера управления на ПЛИС является более гибким, так как логика работы ПЛИС задаётся не при изготовлении, а посредством программирования. Необходимая структура устройства может быть реализована в виде