УДК 681.391

А. Вахаб, асп.; Д.М. Романенко, доц.
(БГТУ, г. Минск)

СТРУКТУРА КЛЮЧА ДЛЯ СТЕГАНОГРАФИЧЕСКОЙ СИСТЕМЫ НА ОСНОВЕ МОДИФИКАЦИИ ЦВЕТОВЫХ ПАРАМЕТРОВ ИЗОБРАЖЕНИЙ

Проблема защиты авторских прав существенно обострилась в связи с вступлением человечества в цифровую эру, где вся информация хранится и передается в цифровом виде. Рассылка документов (текстовых, графических и т.д.) по сети предполагает, что их может получить большое число адресатов. Это также дает возможность недобросовестным пользователям адаптировать или перерабатывать информацию с целью извлечения коммерческой выгоды. Угроза информационного пиратства стала реальностью.

Авторское право распространяется на результаты науки, произведения литературы и искусства, находящиеся в какой-либо объективной форме (в том числе и цифровой):

- письменной (рукопись, машинопись, нотная запись);
- электронной (компьютерная программа, электронная база данных, текст);
- звуко- или видеозаписи (магнитная, оптическая, электронная);
- изображения (картина, рисунок, кино-, теле-, видео-, фотокадр);
- объемно-пространственной (скульптура, макет, сооружение).

Одним из направлений решения указанной проблемы в контексте защиты авторства на объекты в цифровом виде является применение современных стенографических методов.

Цифровая стеганография – направление классической стеганографии, основанное на сокрытии или внедрении дополнительной информации в цифровые объекты, вызывая при этом некоторые искажения этих объектов. В рамках представленного исследования предлагается модификация техники осаждения секретной информации в растровые изображения методом LSB.

Целью модификации является минимизация отклонений цветовых значений модифицированных бит от начальных значений, что позволит достичь большей стегостойкости метода осаждения. Как известно изображение в формате *rgb* по сути представляет собой три массива яркостей пикселей – по одному на каждый канал. Количество

строк и столбцов в массиве соответствует количеству пикселей изобрабражения по горизонтали и вертикали.

$$A_{red} = \begin{vmatrix} a_{0,0} & a_{0,1} & \cdots & a_{0,n-1} \\ a_{1,0} & a_{1,1} & \cdots & a_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m-1,0} & a_{m-1,1} & \cdots & a_{m-1,n-1} \end{vmatrix}, \quad (1)$$

$$A_{green} = \begin{vmatrix} a_{0,0} & a_{0,1} & \cdots & a_{0,n-1} \\ a_{1,0} & a_{1,1} & \cdots & a_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m-1,0} & a_{m-1,1} & \cdots & a_{m-1,n-1} \end{vmatrix}, \quad (2)$$

$$A_{blue} = \begin{vmatrix} a_{0,0} & a_{0,1} & \cdots & a_{0,n-1} \\ a_{1,0} & a_{1,1} & \cdots & a_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m-1,0} & a_{m-1,1} & \cdots & a_{m-1,n-1} \end{vmatrix}. \quad (3)$$

Суть модификации заключается в следующем. На начальном этапе с помощью секретного ключа определяется выборка бит изображения, в которые будет осаждаться секретная информация. Длина выборки равна количеству символов в применяемом алфавите. Так, например, для латинского алфавита, при условии, что выборку осуществляем по красному канала, она может быть следующей (в векторе A' содержатся 26 значения яркостей красного канала, каждая из которых заканчивается на 7).

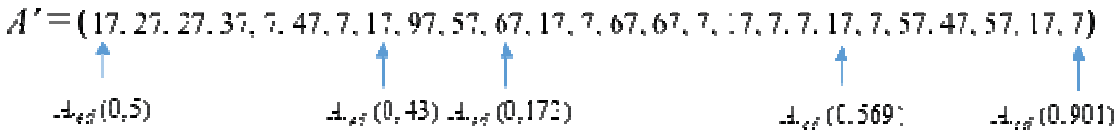

Рисунок 1 – Выборка значений яркости из красного канала

Как видно из рисунка, 26 значения яркости могут быть выбраны из одной строки изображения (значение первого пикселя в выборке равно 17, а его реальный физический адрес в изображении (0,5), а значение последнего пикселя равно 7, а его физический адрес, например, (0, 901), но это не является обязательный условий. Варьировать метод выборки можно будет, задавая соответствующую информацию в стеганографическом ключе.

Количество выборок будет равно количеству осаждаемых символов. В выборку попадают только те биты, младший разряд которых соответствует требованиям ключа. Так, например, в представленном примере предполагалось увеличивать младшие разряды, равные 7, на 1. В таком случае в области осаждения должны быть изначально изменены младшие разряды бит, равные 8 на ближайшее значение, на-

пример, 9. В выборке на 1 увеличивается тот бит, абсолютный номер которого соответствует номеру осаждаемого символа в алфавите. Пусть используем следующий алфавит «ABCDEFGHIJKLMNOPQR STVWXYZ», состоящий из 26 букв. При необходимости осаждения буквы «Н» необходимо на единицу изменить 8-ой бит в выборке, т.е согласно рисунку 1, в массиве значений яркости красного канала пикселю с адресом (0, 43) значение яркости будет изменено с 17 на 18.

Предложенный метод осаждения требует использование составного ключа, состоящего как минимум из следующих параметров.

1. Используемый канал (красный, зеленый, синий) или их комбинация. Суммарно данная часть ключа будет состоять из 4 бит: первый бит соответствует красному каналу, второй – зеленому, третий – синему, а четвертый – альфа-каналу. Единица в разряде канала будет указывать на то, что его нужно использовать при осаждении авторской информации. Так, например, 1000 означает, что для осаждения будет использоваться только красный канал, 1010 – красный и синий.

2. Адрес начального бита выборки. Будут состоять из 32 бит, из которых первые 16 определяют строку изображения для начала выборки, а вторые 16 – номер столбца. Однако если предусмотреть разные отправные точки в выборке бит по разным канал, то суммарно данная часть ключа будет равна 4 × 32 бит. Так, например, если в соответствии с первой частью ключа предусматривается осаждение только в красный канал, т.е. 1000, то первые 32 разряда второй части ключа должны хранить информации о начальном адресе, остальные же разряды заполнены двоичными нулями.

3. Метод формирования выборки, например, из одной строки изображения, или обязательно по одному значению из последовательно идущих разных строк изображения и т.д. Для данного параметра предположительно будет достаточно 8 бит, что соответствует 256 комбинациям.

4. Младший разряд, подлежащий изменению в исходной выборке при осаждении – 4 бита.

5. Математическая операция, применяемая к младшему разряду при осаждении информации – добавление или вычитание единицы. В связи с этим данная часть ключа будет состоять из единственного бита – «0» будет означать, что выполняем вычитание 1, а «1» – наоборот, добавление единицы. Отметим, что сочетание четвертого и пятого пункта определяем маскирующий бит, который в зоне выборки должен быть предварительно изменен на 1.

Секретный ключ может быть расширен и дополнительными параметрами, например, количеством повторений операции осаждения и т.д.

В заключении необходимо отметить, что предложенный метод позволяет осаждать секретную информацию, при этом начальные значения пикселей будет изменяться только лишь на 1, что должно повысить стегостойкость контейнера.

ЛИТЕРАТУРА

1. Urbanovich, N. The use of steganographic techniques for protection of intellectual property rights / N. Urbanovich, V. Plaskovitsky // Electrical Review (Przeglad elektrotechniczny). – 2012. – № 11b. – S. 342–344.

2. Романенко, Д.М. Методы цифровой стеганографии на основе модификации цветовых параметров изображения / Д. М. Романенко, Алаа Вахаб // Труды БГТУ. – 2018. – № 1 (206). – С. 94–99.

УДК 003.26 +347.78

Р.И. Белькевич, асп.; Д.М. Романенко, доц.
(БГТУ, г. Минск)

ОСОБЕННОСТИ РАЗРАБОТКИ ИМИТАЦИОННОЙ МОДЕЛИ ПРОЦЕССА ЗАЩИТЫ ПЕРЕДАВАЕМЫХ ПО ДВОИЧНЫМ КАНАЛАМ ДАННЫХ НА ОСНОВЕ МНОГОМЕРНОЙ ПОСЛЕДОВАТЕЛЬНО-ПАРАЛЛЕЛЬНОЙ СХЕМЫ КОДИРОВАНИЯ

В рамках данной работы предполагается, что применение последовательно-параллельных методов кодирования и декодирования положительно скажется на возможность исправления ошибок, возникающих во время передачи бинарной последовательности. Для проверки этого предположения необходимо реализовать систему передачи данных, состоящую из двух модулей:

- Кодер
- Декодер

Разрабатываемый кодер является сложной системой, состоящей из множества составных частей. Из основных компонентов можно перечислить модуль кодера, модуль имитации передачи и модуль декодера. Из вспомогательных модулей необходимо реализовать модули построения трехмерной структуры, модуль формирования бинарной строки , модуль параллельной обработки, модуль параллельной обработки ошибок и модуль анализа результатов.

Схема всей системы представлена на рисунке 1.

Модуль построения трехмерной структуры решает задачу по преобразованию одномерной строки входных бинарных данных в