2. Бердышев, А.В. Об условиях развития банков в цифровой экономике / А.В. Бердышев. – Краснодар, 2018. – С. 395.

3. Garg, A. Analytics in banking: Time to realize the value / A. Garg, D. Grande. – [Electronic resource], www.mckinsey.com, 2018. – С. 395.

4. Бутенко, Е.Д. Искусственный интеллект в банках сегодня: опыт и перспективы / Е.Д. Бутенко // Финансы и кредит. – 2018. – № 5 (773) – С. 143.

УДК 003.26+347.78

А. Вахаб, асп.; Д. М. Романенко, зав. каф. ИиВД (БГТУ, г. Минск)

СТЕГАНОГРАФИЧЕСКАЯ СИСТЕМА ДЛЯ ВНЕДРЕНИЯ АВТОРСКОЙ ИНФОРМАЦИИ В РАСТРОВЫЕ ИЗОБРАЖЕНИЯ

В современном цифровом мире по компьютерной сети передается любая информация. Это стало неотъемлемой частью нашей жизни. При этом может стоять задача секретной передачи, «не видимой» для посторонних людей или программ, причем скрывается сам факт передачи информации, или внедрение секретной (авторской) информации в какой-либо цифровой контейнер, например, изображение. Для решения данного круга задач могут быть использованы методы стеганографии. Цифровая стеганография – направление классической стеганографии, основанное на сокрытии или внедрении дополнительной информации в цифровые объекты, вызывая при этом некоторые искажения этих объектов.

Формальное описание разрабатываемой стеганографической системы основывается на учете взаимодействия компонентов системы, которые, в общем случае задаются элементами соответствующих множеств [1]: сообщения M ($M \in M$, M – множество всех сообщений); контейнера C ($C \in C$, C – множество всех контейнеров); ключа K ($K \in K$, K – множество всех ключей); заполненного контейнера (или стегосообщения) S ($S \in S$, S – множество всех стегосообщений).

В таком случае стеганографический алгоритм составляют два преобразования, задаваемые на основе отображений:

1) прямое стеганографическое преобразование F, сопоставляющее сообщению, пустому контейнеру, ключу заполненный контейнер:

$$M \times C \times K \rightarrow S; \quad (1)$$

2) обратное стеганографическое преобразование F^{-1}, сопоставляющее заполненному контейнеру и ключу исходное сообщение M:

$$S \times K \rightarrow M. \quad (2)$$

Причем

$$F(M, C, K) = S, \quad (3)$$

$$F\text{-}1 = (S, K) = M, \quad (4)$$

где $M \in \boldsymbol{M}$, $C \in \boldsymbol{C}$, $K \in \boldsymbol{K}$, $S \in \boldsymbol{S}$.

Под стеганографической системой будем понимать систему, формально описываемую выражением вида:

$$\Sigma = (F, F^{-1}, M, C, K), \quad (5)$$

и представляющую собой совокупность сообщений, секретных ключей, контейнеров и связывающих их преобразований.

Под внедрением (скрытием) сообщения с помощью системы Σ в контейнер C понимают применение прямого стеганографического преобразования F к конкретным M, C и K. Извлечение сообщения по сути представляется, как применение обратного стеганографического преобразования F^{-1} с теми же значениями аргументов, что и при скрытии сообщения.

Предлагаемая стеганографическая система основывается на принципиально новом методе прямого стеганографического преобразования F растровых изображений, который отличается от известных методов, например, LSB, минимальными отклонениями значений пикселей модифицированного и исходного контейнера [2].

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 изображения по горизонтали и вертикали.

$$A_{red} = \begin{vmatrix} a_{0,0} & a_{0,1} & \cdots & a_{0,n-1} \\ a_{1,0} & a_{1,1} & \cdots & a_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m-1,0} & a_{m-1,1} & \cdots & a_{m-1,n-1} \end{vmatrix}, \quad (6)$$

$$A_{green} = \begin{vmatrix} a_{0,0} & a_{0,1} & \cdots & a_{0,n-1} \\ a_{1,0} & a_{1,1} & \cdots & a_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m-1,0} & a_{m-1,1} & \cdots & a_{m-1,n-1} \end{vmatrix}, \quad (7)$$

$$A_{blue} = \begin{vmatrix} a_{0,0} & a_{0,1} & \cdots & a_{0,n-1} \\ a_{1,0} & a_{1,1} & \cdots & a_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m-1,0} & a_{m-1,1} & \cdots & a_{m-1,n-1} \end{vmatrix}. \quad (8)$$

Суть предлагаемой модификации заключается в следующем. На начальном этапе с помощью секретного ключа определяется выборка бит изображения, в которые будет осаждаться информация. Длина выборки для осаждения одного символа равна количеству символов в применяемом алфавите. Так, например, для латинского алфавита, при условии, что выборку осуществляем по красному каналу, она может быть следующей (в векторе A_1' содержатся 26 значения яркостей красного канала, каждая из которых заканчивается на 7 (данная цифра определяется ключом).

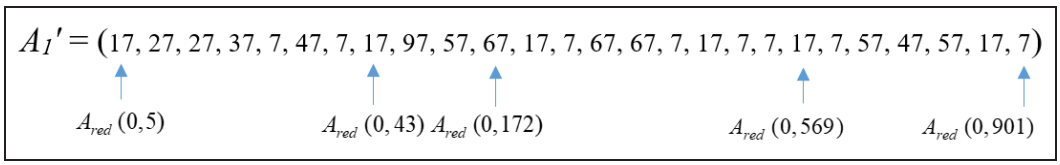

Рисунок 1 – Выборка значений яркости из красного канала

Как видно из рисунка 1, 26 значений 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 обязательным условием. Правила формирования выборки могут также задаваться ключом.

В целом для каждого осаждаемого бита формируется соответствующая выборка (вектор) A_1', A_2', A_3'... A_k', где k – количество осаждаемых символов, которые в итоге записываются в вектор следующего вида:

$$A' = [A_1', A_2', A_3', \dots A_k']. \tag{9}$$

При осаждении первого символа в выборке A_1' на 1 увеличивается бит с адресом (1, *num*), где *num* соответствует номеру осаждаемого символа в алфавите (нумерацию строк, равно как и столбцов в матрице A' для упрощения будем начинать не с 0, а с 1). Пусть используем следующий алфавит «ABCDEFGHIJKLMNOPQRSTVWXYZ», состоящий из 26 букв. При необходимости осаждения буквы «H» на единицу будет изменяться элемент матрицы $A'(1, 8)$, другими словами 8-ой бит в выборке A_1'. Поэтому согласно рисунку 1, в массиве значений яркости красного канала пикселю с адресом (0, 43) значение яркости будет изменено с 17 на 18. Аналогичные операции выполняются и для остальных строк массива A', т.е. для каждой из подготовленных выборок.

Далее рассмотрим общий вид ключа (K) стеганографической системы, который будет состоять как минимум из следующих блоков, представленных в десятичном виде.

1. Блок K^1, определяющий используемые для осаждения каналы (красный, зеленый, синий, альфа-канал) или их комбинацию. Суммарно данная часть ключа будет состоять из 4 символов: символ «#» означает, что данный канал не используется при осаждении, а одно из значений в диапазоне {0-9} означает, что именно значения яркости с данным младшим битом будут попадать в выборки A_1', A_2', A_3'... A_k' и в дальнейшем модифицироваться. Причем первый символ соответствует красному каналу, второй – зеленому, третий – синему, а четвертый – альфа-каналу. Так, например, K^1=7### означает, что для осаждения будет использоваться только красный канал и выбираться будут значения, заканчивающиеся на 7 (как было показано на рисунке 1), а K^1=7#5# – в красном канале используем значения яркости с младшим битом равным «7», а в синем канале – равном «5».

2. Адрес начального бита выборки (K^2). Будут состоять из 32 бит, из которых первые 16 определяют строку изображения для начала выборки, а вторые 16 – номер столбца матрицы изображения. Однако если предусмотреть разные отправные точки в выборке бит по разным каналам, 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, например, K^1=7###, то первые 32 разряда блока K^2 должны хранить информации о начальном адресе, остальные же разряды (3×32) заполнены двоичными нулями.

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

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

ЛИТЕРАТУРА

1. Шутько, Н. П. Математическая модель системы текстовой стеганографии на основе модификации пространственных и цветовых параметров символов текста / Н. П. Шутько, Д. М. Романенко, П. П. Урбанович // Труды БГТУ. Сер. VI: Физ.-мат. науки и информатика. – 2015. – № 6. – С. 152–156.

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.