with anchor). The neural network computes the 128-d embeddings for each face and then tweaks the weights of the network.

On the recognition stage, we can see the face on the camera, and if the person was photographed and trained earlier, our Recognizer will do a «processing» that returns its ID and index, which shows how confident the Recognizer is in this feature.

REFERENCES

1 Face Detection using Haar Cascades [Electronic resource] / link https://docs.opencv.org/3.3.0/d7/d8b/tutorial_py_face_detection.html / Date of access: 08.09.2020

2 Cascade Classifier Training [Electronic resource] / link https://docs.opencv.org/3.3.0/dc/d88/tutorial_traincascade.html / Date of access: 08.09.2020

А.ВАХАБ[1], Д.М.РОМАНЕНКО[1]

МАТРИЧНЫЙ МЕТОД ОСАЖДЕНИЯ ИНФОРМАЦИИ В РАСТРОВЫЕ ИЗОБРАЖЕНИЯ НА ОСНОВЕ МОДИФИКАЦИИ ЦВЕТОВЫХ ПАРАМЕТРОВ

[1]Учреждение образования «Белорусский государственный технологический университет», г. Минск, Республика Беларусь

При постановке задачи секретной передачи, «не видимой» для посторонних людей или программ, при скрытии самого факта передачи информации, или внедрения секретной (авторской) информации в какой-либо цифровой контейнер, 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. В рамках представленного исследования предлагается разработка техники осаждения информации в растровые изображения по аналогии с методом LSB [1]. При этом главной отличительной особенностью предлагаемой техники осаждения 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 изображения по горизонтали и вертикали.

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

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

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

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).

$$A_1' = (17, 27, 27, 37, 7, 47, 7, 17, 97, 57, 67, 17, 7, 67, 67, 7, 17, 7, 7, 17, 7, 57, 47, 57, 17, 7)$$

$A_{red}(0,5)$ $A_{red}(0,43)$ $A_{red}(0,172)$ $A_{red}(0,569)$ $A_{red}(0,901)$

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 двумерную матрицу следующего вида:

$$A' = \begin{bmatrix} A_1' \\ A_2' \\ A_3' \\ \\ A_k' \end{bmatrix}. \qquad (4)$$

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 «Н» 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.

Предложенный метод осаждения для реализации вариативности требует использование стеганографического ключа, состоящего 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. 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.