Волченко М.В., Цыкал А.О.

Институт информатики и искусственного интеллекта ДонНТУ

О способе повышения криптоустойчивости алгоритма lsb

В настоящей работе рассматривается проблема скрытия текстового сообщения в изображении формата .bmp без заметных человеческому глазу искажений, которая находит широкое применение в таких областях как защита личной тайны, цифровые водяные знаки, электронная цифровая подпись и электронная торговля [1].

Существует большое число методов сокрытия текстовой информации в изображении [2]. Одним из наиболее широко используемых и эффективных является метод LSB (Least Significant Bits) или метод замены младших битов [3]. Идея метода заключается в замене от одного до четырех младших битов в байтах цветового представления точек исходного изображения битами скрываемого сообщения. Возможность такой замены обусловлена некоторой избыточностью представления цвета и возможным случайным поведением младших битов.

Обычно, в качестве контейнера используется BMP-изображение, которое для хранения цвета пикселя использует формат RGB (Red, Green, Blue) а для хранения значения каждого из них использует 8 бит (256 оттенков). Изменение последних битов изображения, в виду особенностей зрения, не заметно человеку, но позволяет аддитивно записывать любую информацию в битовом представлении [2].

Недостатком такого представления является то, что скрываемая информация, записывается последовательно, т. е. если найти начало сообщения остальное сразу становиться доступным, что существенно снижает криптоустойчивость [3].

Цель настоящей работы – разработать способ записи скрываемой информации в изображении для алгоритма LSB с целью повышения его криптоустойчивости.

Авторами предлагается использовать секретный ключ для вычисления бита изображения, в который будет произведена запись. Для большей защиты такой ключ будет использоваться для получения шифротекста по исходному изображению, который и будет помещаться в изображение.

Предложенный в данной работе модифицированный алгоритм LSB состоит в шифровании исходного сообщения, переводе шифротекста в бинарный код, записи такого кода в исходное изображение.

Исходные данные:

– изображение формата BMP;

– *message* – скрываемый текст сообщения;

– *Key* – секретный ключ.

Ограничения:

Длина *K* сообщения *message* не должна превышать количество пикселей:

$$K < Sh * h ,$$

где *K* – длина сообщения *message*, *Sh* – ширина изображения, *h* – высота изображения.

Выходные данные:

– изображение формата BMP, содержащее скрытый шифротекст.

1. Шифрование исходного сообщения

Для представления текстовой информации используется кодировка Windows-1251, как стандартная кодировка всех Windows-приложений. В такой кодировке каждому символу соответствует определенное значение от 0 до 255. Поэтому локальный ключ алгоритма вычисляется по формуле:

$$Key = \sum_{0}^{K}(message_i * Key) \bmod 255 ,$$

Если $Key \bmod 5 = 0$, то $Key = Key - 1$.

Если $Key = 0$, то $Key = 1$.

В качестве алгоритма шифрования может быть выбран любой асимметричный криптоалгоритм. В настоящей работе был выбран один из наиболее простых и популярных алгоритмов – шифр Цезаря, в котором каждый символ в открытом тексте заменяется буквой, находящейся на некотором постоянном числе позиций левее или правее него в кодировке. Шифротекст определяется по формуле:

$$New_i = (\Pr ev_i - Key) \bmod 255 ,$$

где $i=1...K$, New_i – i-ый символ шифротекста, $\Pr ev_i$ – i-ый символ открытого текста.

2. Запись сообщения в изображение

Координаты пикселя для записи очередного символа шифротекста определяются по формуле:

$$X_i = (j * Key) \bmod Sh ; \quad Y_i = (j * Key * X_i) \bmod h ;$$

где X_i – координата пикселя по ширине, Y_i – координата пикселя по высоте, $i=0...K$, $j=1...K+1$.

Для записи сообщения в изображение необходимо перевести шифротекст и значения оттенков цветов пиксела с координатами (X_i , Y_i) в двоичный формат. В результате такого перевода получим 4 различных байта: m – двоичное представление шифротекста New, r,g,b – двоичные представления красной, зеленой и синей составляющих пиксела с координатами (X_i , Y_i). Далее происходит запись битового кода шифротекста в определенные биты оттенков по формулам:

$$r_7 = m_0 , r_6 = m_1 , g_7 = m_2 , g_6 = m_3 ,$$

$$g_5 = m_4 , b_7 = m_5 , b_6 = m_6 , b_5 = m_7 ,$$

В результате таких преобразований будет получено новое изображение в формате bmp, содержащее скрытый шифротекст сообщения, которое и будет передаваться по открытому каналу связи.

3. Восстановление исходного сообщения

Считывание сообщения из переданного изображения заключается в определении шифротекста по формулам:

$$m_0 = r_7 \text{ , } m_1 = r_6 \text{ , } m_2 = g_7 \text{ , } m_3 = g_6 \text{ ,}$$

$$m_4 = g_5 \text{ , } m_5 = b_7 \text{ , } m_6 = b_6 \text{ , } m_7 = b_5$$

и получения исходного сообщения с помощью дешифрования:

$$m = (\, m + Key) \bmod 255 \text{ .}$$

В настоящей работе предложен новый способ записи скрываемого сообщения в изображении, что позволило преодолеть проблему последовательного заполнения битов изображения и, следовательно, повысить, криптоустойчивость системы. Наибольшая эффективность предложенного алгоритма была достигнута при кодировании сообщений длиной не большее 40% от числа пикселей изображения.

Литература.

1. Грибунин В.Г. Цифровая стеганография / Грибунин В.Г., Оков И.Н., Туринцев И.В. – М. : Солон-Пресс, 2002. – 272 с.

2. Барсуков В.С. О Кустов В. Н., Федчук А. А. Методы встраивания скрытых сообщений // Защита информации. Конфидент. – 2002. – №3. – 34-37 с.

3. Алиев А.Т. О применении стеганографического метода LSB к графическим файлам с большими областями монотонной заливки / А.Т. Алиев // Вестник ДГТУ. – Ростов-на-Дону, 2004. – Т. 4, № 4 (22). – С. 454-460.