УДК 681.323(075)

**А.А. Курная,**

**А. С. Кочубей**

(Тихоокеанский государственный университет, г. Хабаровск)

**СОКРЫТИЕ ДАННЫХ В ЗАШИФРОВАННЫХ ИЗОБРАЖЕНИЯХ, ИСПОЛЬЗУЮЩЕЕ** **MSB ПРЕДСКАЗАНИЕ**

*Ключевые слова:* обратимое сокрытие данных, MSB предсказание (MSB – наиболее значащий бит), ключ шифрования, ключ сокрытия данных, объем внедрения

В статье рассматриваются два различных подхода к обратимому сокрытию данных в зашифрованных изображениях, использующих MSB предсказание. Они обеспечивают внедрение большого объема информации (до двух бит на пиксель) при высоком качестве внедрения и извлечения, а также позволяют полностью восстановить исходное изображение.

Безопасность цифровых изображений играет значительную роль во всех областях, особенно в таких высокочувствительных как медицина и военное дело. Поэтому защита изображений в последние годы, в связи с интенсивным развитием информационных технологий и облегчением доступа к передаваемой информации, привлекает особое внимание специалистов. Предложено множество методов, технологий для защиты изображений во время их передачи и хранения.

Защитить изображение, установить его авторство, подтвердить целостность можно путем внедрения в него секретной информации с последующим ее извлечением. Этим занимается такой раздел стеганографии как цифровое маркирование. Для дополнительной защиты можно использовать шифрование как самого изображения, так и внедряемой в него информации, а это уже раздел криптографии.

Таким образом, распространение получили методы сокрытия данных в зашифрованных изображениях, основывающиеся как на положениях стеганографии, так и криптографии.

Методы сокрытия данных, в основе которых лежит MSB предсказание, используют то обстоятельство, что яркости соседних пикселей изображения, как правило, практически не отличаются или отличаются друг от друга незначительно, что позволяет предсказывать утерянные значения.

В работе [1] французских исследователей предлагается обратимый алгоритм сокрытия данных в зашифрованных изображениях, позволяющий внедрять секретное сообщение (один бит на пиксель) подстановкой в MSB.

В работе [2] индийских исследователей рассматривается метод, позволяющий внедрять секретное сообщение уже заменой двух бит MSB. Поскольку значения замененных MSB теряются на этапе сокрытия данных, необходимо уметь безошибочно предсказывать их на этапе декодирования.

Предлагаются два подхода к решению задачи обратимого сокрытия данных в зашифрованных изображениях – высокообъемное обратимое сокрытие данных в наиболее значимых битах (MSB) с коррекцией ошибок предсказания (первый подход) и высокообъемное обратимое сокрытие данных в MSB с внедряемыми ошибками предсказания (второй подход).

При первом подходе все ошибки предсказания корректируются перед шифрованием. На этапе дешифрирования исходное изображение полностью восстанавливается, но секретное сообщение искажается.

При втором подходе исходное изображение непосредственно шифруется, но после шага шифрования внедряется информация о местоположении ошибок.

В обоих подходах MSB каждого доступного пикселя заменяются в зашифрованном изображении двумя битами секретного сообщения. После этого выполняется декомпрессия сжатого изображения, внедренные данные извлекаются без каких-либо ошибок, а исходное изображение восстанавливается без потерь с помощью MSB предсказания.

На рис. 1, 2 представлены укрупненные схемы алгоритмов, соответствующие каждому из подходов.

Как видно из рис. 1, фаза кодирования включает четыре этапа:

* определение ошибки предсказания;
* шифрование изображения;
* внедрение двух битов MSB подстановкой;
* сжатие.

На фазе декодирования действия выполняются в обратном порядке. Сначала выполняется декомпрессия маркированного зашифрованного изображения, затем осуществляются извлечение секретного сообщения и восстановление исходного изображения.

Предварительная обработка

Шифрование изображения

Сжатие

Декомпрессия

Расшифровка изображения

Предсказание старшего значащего бита

Извлечение значения из старшего значащего бита

Расшифровка данных

Входное изображение

Обнаружение ошибки предсказания

База данных

Сокрытие данных в двух старших значащих битах

Шифрование данных

Двоичная карта местоположения ошибки

Ключ шифрования

Ключ сокрытия данных

Секретные данные

Ключ шифрования данных

Ключ шифрования

Секретные данные

Ключ сокрытия данных

Восстановленное изображение

Рис.1 Укрупненная схема алгоритма высокообъемного обратимого сокрытия данных в MSB с коррекцией ошибок предсказания (первый подход)

Рассмотренные подходы к решению задачи сокрытия данных в зашифрованных изображениях находятся на стадии программной реализации, которая выполняется в рамках ВКР (первый подход – Курная А.А., второй – Кочубей А.С.). В дальнейшем предполагается исследование алгоритмов на эффективность и их сравнительный анализ.

Шифрование изображения

Внедрение информации о местоположе-нии ошибок

Сжатие

Декомпрессия

Расшифровка изображения

Предсказание старших значащих битов

Извлечение значений из старших значащих битов

Расшифровка данных

Входное изображение

Обнаружение ошибки предсказания

База данных

Сокрытие данных в двух старших значащих битах

Шифрование данных

Бинарная карта локализации ошибок

Ключ шифрования

Ключ сокрытия данных

Секретные данные

Ключ шифрования данных

Ключ расшифровки

Секретные данные

Ключ сокрытия данных

Восстановленное изображение

Рис.2 Укрупненная схема алгоритма высокообъемного обратимого сокрытия данных в MSB с внедренными ошибками предсказания (второй подход)

Программы, реализующие данные подходы, смогут полноценно использоваться в цифровом маркировании изображений для внедрения больших объемов секретной информации и при этом обеспечат высокое качество маркированного изображения, извлеченной информации, а также позволят полностью восстанавливать исходное изображение, что является очень важным моментом в некоторых приложениях.

**Список используемых источников**

1. *Pauline Puteaux, and William Puech,* “An Efficient MSB Prediction-Based Method for High-Capacity Reversible Data Hiding in Encrypted Images” IEEE Transactions on Information Forensics and Security, 2018.
2. *Aswathy Lekshmi.S., Hari.S, Netha Merin Mathew* “High Capacity Reversible Data Hiding in Encrypted Images by MSB Prediction Method” International Research Journal of Engineering and Technology (IRJET), Volume: 06 Issue: 04| Apr 2019.

**G.I. Bakhrushina,**

**A.A. Kurnaya,**

**A.S. Kochubey,**

**A.P. Bakhrushin**

**DATA HIDING IN ENCRYPTED IMAGES USING MSB PREDICTION**

*Keywords: reversible data hiding, MSB prediction (MSB – most significant bit), encryption key, data hiding key, embedding capacity.*

The article describes two different approaches for the reversible data hiding in encrypted images, using MSB prediction. It is possible to hide two bits per pixel and in addition to get high quality of data embedding/extracting. Besides, these approaches give the possibility of perfectly reconstructing of the original image.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

© Бахрушина Г.И., 2020

© Курная А.А., 2020

© Кочубей А.С., 2020

© Бахрушин А.П., 2020