УДК 004.056.55

ИССЛЕДОВАНИЕ И ОЦЕНКА КАЧЕСТВА АЛГОРИТМОВ ЗАЩИТЫ 3D-ИЗОБРАЖЕНИЙ

***Р.С. СМИРНОВ*[1*], *Н.А. МАСЛОВА*[2]**

[1] *магистрант кафедры прикладной математики и информатики, ДонНТУ, Красноармейск, УКРАИНА*

[2] *доцент кафедры прикладной математики и информатики, канд. техн. наук, ДонНТУ, Красноармейск, УКРАИНА*

[*] *email: russ944@mail.ru*

На сегодняшний день вопрос анализа и применения алгоритмов защиты программ и данных является актуальным. На всех предприятиях есть конфиденциальная информация, которая должна быть защищена и доступ к данным могут получить только субъекты, имеющие на нее право. Для этого необходимо обеспечить защиту данных, используя различные алгоритмы шифрования и обеспечения безопасности. В области изображений это защита от несанкционированного копирования, контроль соответствия изображения эталону, определение автора и источника 3D-модели, а, в конечном счете, проверка надежности и целостности данных, составляющих изображение.

Алгоритмы защиты могут быть применены к графическим файлам в различных приложениях, например, к 3D-изображениям в пакетах графического моделирования, к фото- и видеоматериалам, схемам, рисункам и иллюстрациям. Надежность встраиваемых в различные графические объекты средств защиты может быть подвергнута пользователем сомнению либо отсутствовать вовсе. Задачами работы является анализ существующих алгоритмов защиты изображений; исследование возможных методов шифрования данных; создание комплексного алгоритма, который обеспечит многоступенчатую защиту изображений, включая защиту от копирования, электронную подпись, и стеганографическую надпись; программного продукта, который продемонстрирует защиту на примере 3D-изображений ландшафта.

Рассмотрим упомянутые методы подробнее. Опишем создание электронной подписи с использованием асимметричной схемы шифрования [1].

1. Генерация ключевой пары. Из множества случайно выбирается закрытый ключ и вычисляется соответствующий ему открытый ключ.
2. На основе закрытого ключа вычисляется подпись.
3. Верификация подписи. Для данного электронного документа определяется действительность подписи, используя открытый ключ.

В качестве ассиметричного алгоритма берется алгоритм RSA, суть которого заключается в следующем. Вначале вычисляется закрытый ключ и открытый ключ. Для этого отправителем документа выбираются два больших простых числа p и q, находится их произведение: $N = p * q$, и значение функции

$f(N) = (p - 1)(q - 1)$. Далее отправитель вычисляет число E такое, что: $E <= f(N)$, $НОД(E, f(N)) = 1$; а также число D: $D < N$, $E * D$.

Пара чисел E и N – открытый ключ, который отправитель дает получателю для последующей проверки его подписи. Число D является закрытым ключом и применяется отправителем для подписи. Общая схема формирования и проверки цифровой подписи RSA приведена на рис. 1, m – это передаваемое сообщение, которое может встраиваться в изображение.

Рис. 1 – Схема цифровой подписи RSA

Еще одной частью защиты изображения является стеганографический метод (цифровой водяной знак – ЦВЗ) – технология, созданная для защиты авторских прав мультимедийных файлов, и, в частности, изображений [2].

Опишем формальное представление генерации ЦВЗ в виде математической модели. Пусть $Y_{ЦВЗ}$ – множество ЦВЗ, $X_{ключ}$ – множество ключей, $X_{блок}$ – множество блоков, $X_{сообщ}$ – множество сообщений. Тогда генерация ЦВЗ имеет вид (1):

$$Y_{ЦВЗ} = F(X_{блок}, X_{ключ}, X_{сообщ}), \quad (1)$$

Сам процесс внедрения ЦВЗ в изображение с $X_{маска}$ – маска внедрения, выбирающаяся с учетом заметности ЦВЗ можно описать так (1):

$$\Psi: X_{блок} \times Y_{ЦВЗ} \times X_{маска} \rightarrow X_{зап.\ блок}, \quad (2)$$

Схема внедрения сообщения имеет следующий вид (рис. 2).

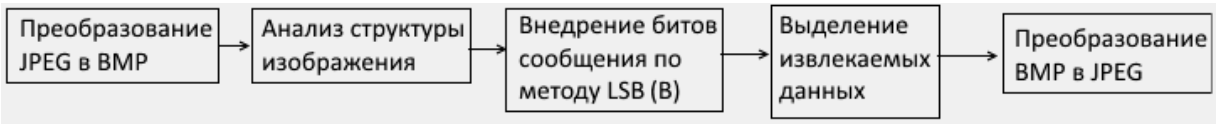

Рис. 2 – Схема внедрения ЦВЗ

Суть метода LSB (B) в том, что внедрение битов происходит в B-составляющий цвета, поскольку человеческий глаз хуже отличает изменения синего цвета. Итогом работы является не только исследование, но и практическое предложение по защите изображений. Комплексный алгоритм предназначен для многоступенчатой защиты и включает защиту от копирования, электронную подпись и авторский цифровой знак.

Список литературы:

1. *Рябко Б.Я.* Основы современной криптографии. / *Б.Я. Рябко, А.Н. Фионов* // Научный Мир. – 2004. – 173 с.

2. *Сидоркина И.Г.* Алгоритм распознавания трехмерных изображений с высокой детализацией / *И.Г. Сидоркина, А.Г. Коробейников, П.А. Кудрин* // Вестник Марийского государственного технического университета. – 2010. – № 2 (9). – С. 91-99.