ностей педагогических вузов. При этом аргументируется данная ситуация тем, что на современном этапе все традиционные технические средства обучения успешно заменил компьютер. Однако к современным средствам обучения относятся мультимедиа-проектор, сканер, графический планшет, интерактивная доска. В недалеком будущем в школах будет применяться такое средство обучения, как электронный планшет, который придет на смену традиционным учебникам. Необходимость квалифицированного подхода к современным техническим средствам обучения со стороны будущих преподавателей очевидна, так как невозможно каждого педагога обеспечить компетентным в обслуживании данных устройств помощником. Реальность же такова, что у студентов возникают проблемы при применении мультимедиа-средств на этапе подготовки и в процессе их использования. Решение этой проблемы видится в том, чтобы включить в состав дисциплины «Основы информационных технологий» теоретическую и практическую составляющие изучения технических средств обучения. Поэтому в рамках преподаваемой дисциплины было уделено особое внимание овладению навыками грамотного обращения с разнообразной мультимедиа-техникой. Студенты практиковались в умении подключать, настраивать, устранять мелкие неполадки оборудования. Проведение таких занятий сократило время на подготовку к представлению презентаций и способствовало активизации использования технических средств обучения, а также позволило чувствовать себя уверенно при работе с ними.

УДК 004.921

ПРИМЕНЕНИЕ СТЕГАНОГРАФИИ ДЛЯ ЗАЩИТЫ АВТОРСКОГО ПРАВА ФОТОГРАФИЙ В ФОРМАТЕ JPEG

Савлевич Ю.И.

УО «Витебский государственный университет им. П.М. Машерова», г. Витебск
Научный руководитель – Савельева Н. В., к. ф.- м. н.

В последнее время в мире становится всё актуальнее проблема пиратства, и, как следствие, защиты информации от несанкционированного использования. Особенно данная проблема актуальна для цифровых данных. Цифровая информация подвержена незаконному копированию, что мешает её создателям получать прибыль и продолжать развивать свои идеи. Вопрос безопасности информации и защиты авторских прав напрямую касается и пользователей цифровых фотокамер, желающих защитить свои фотографии, которые могут стать для них источником заработка.

Основная цель настоящей работы – разработка метода защиты авторского права на цифровые фотографии в формате JPEG посредством внесения в изображение дублирующей метки с информацией о пользователе и камере.

В цифровой фотографии существуют информационные поля, например, время, дата, модель фотоаппарата, которым сделан снимок. Но эти поля можно легко изменить, что подвергнет сомнению авторство фотоснимка. Таким образом, предлагается использовать поле цифрового снимка «данные», которое недоступно для изменения пользователю напрямую. Для модификации этого поля можно использовать стеганографические алгоритмы, комбинируя их с алгоритмами шифрования. На наш взгляд, целесообразно дублировать информацию о снимке из доступных для редактирования полей непосред-

ственно в поле «данные» изображения с целью последующего сравнения для заключения о том, менялась ли информация о фотоснимке.

Рассмотрим подробнее формат JPEG [1]. Алгоритм JPEG (см. рис. 1) позволяет сжимать изображение как с потерями, так и без потерь. Но поскольку режим сжатия без потерь используется крайне редко, то ограничимся рассмотрением режима со сжатием.

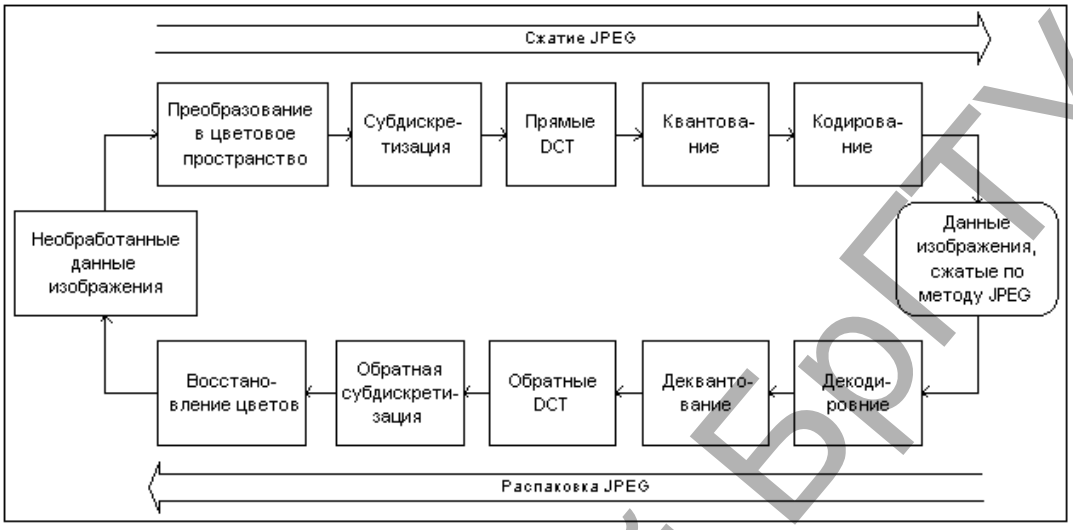

Рисунок 1 – Алгоритм сжатия JPEG

При сжатии изображение преобразуется из цветового пространства RGB в YCbCr, после чего для каналов изображения Cb и Cr, отвечающих за цвет, может выполняться т.н. прореживание, когда каждому блоку из 4 пикселов (2x2) яркостного канала Y ставятся в соответствие усреднённые значения Cb и Cr (схема прореживания "4:2:0"). При этом для каждого блока 2x2 вместо 12 значений (4 Y, 4 Cb и 4 Cr) используется всего 6 (4 Y и по одному усреднённому Cb и Cr). Если к качеству восстановленного после сжатия изображения предъявляются повышенные требования, прореживание может выполняться лишь в каком-то одном направлении – по вертикали (схема "4:4:0") или по горизонтали ("4:2:2"), или не выполняться вообще ("4:4:4").

Далее яркостный компонент Y и отвечающие за цвет компоненты Cb и Cr разбиваются на блоки 8x8 пикселов, и каждый блок подвергается дискретному косинусному преобразованию (ДКП). Полученные коэффициенты ДКП квантуются (для Y, Cb и Cr в общем случае используются разные матрицы квантования) и пакуются с использованием кодов Хаффмана [2]. Матрицы, используемые для квантования коэффициентов ДКП, хранятся в заголовочной части JPEG-файла и обычно строятся так, что высокочастотные коэффициенты подвергаются более сильному квантованию, чем низкочастотные. Это приводит к огрублению мелких деталей на изображении (чем выше степень сжатия, тем более сильному квантованию подвергаются все коэффициенты).

При сохранении изображения в JPEG-файле указывается параметр качества, задаваемый в некоторых условных единицах, например, от 1 до 100 или от 1 до 10. Большее число обычно соответствует лучшему качеству (и большему размеру сжатого файла). Однако даже при использовании наивысшего качества (соответствующего матрице квантования, состоящей из одних только единиц) восстановленное изображение не будет в точности совпадать с исходным, что связано как с конечной точностью выполнения ДКП, так и с необходимостью округления значений Y, Cb, Cr и коэффициентов ДКП до ближайшего целого.

Для сокрытия информации об авторе фотографии нами выбран *метод сокрытия в спектре изображения после квантования* [3], который основан на использовании частот блоков изображения после их квантования, но перед этапом кодирования. При этом сокрытие может осуществляться при помощи классических методов компьютерной стеганографии. При использовании данного метода объем скрываемых данных пропорционален объему сжатого изображения, при этом увеличение объема внедряемой информации может приводить к изменениям исходного изображения и снижению эффективности последующего этапа кодирования. Однако возможность варьировать качество сжатого изображения в широком диапазоне не позволяет легко установить, являются ли возникающие в результате сжатия погрешности следствием сокрытия данных или использования больших коэффициентов квантования.

Приведем краткое описание данного метода. Пусть m_j – биты скрываемого сообщения, $B_{i,j}$ – значения ненулевых элементов блоков квантованного спектра немодифицированного изображения, упорядоченные согласно порядку их кодирования в алгоритме JPEG (i – номер бита элемента, j – номер элемента), $B'_{i,j}$ – соответствующие блоки модифицированного изображения. Введем двоичную последовательность k_j, биты которой поставим в соответствие блокам $B_{i,j}$, при этом k_j=1, если в младший бит j-го блока скрывается очередной бит сообщения, и k_j=0 в противном случае.

Прямое и обратное стеганографическое преобразование $F{:}M\times B\times K\to B$ и F^{-1}: $B\times K\to M$ для данного метода имеют вид (1) и (2) соответственно:

$$B'_{i,j}=\begin{cases} B_{i,j}, \text{если } i\neq 0 \\ B_{i,j}, \text{если } i=0 \text{ и } k_j=0 \\ m_l, \text{если } i=0 \text{ и } k_j=1, \text{где } l=\sum_{p=1}^{j}k_p \end{cases} \qquad j=1,2,3,... \tag{1}$$

$$m_j=B'_{0,l}, \text{где } l \mid \sum_{p=1}^{l}k_p=j \mid j=1,2,3,... \tag{2}$$

Для обеспечения высокой степени безопасности внедряемую метку будем кодировать шифром сложной замены [4]. Напомним, что шифры сложной замены называют многоалфавитными, т.к. для шифрования каждого символа исходного сообщения применяют свой шифр простой замены. Многоалфавитная подстановка последовательно и циклически меняет используемые алфавиты. При r-алфавитной подстановке символ x_0 исходного сообщения заменяется символом y_0 из алфавита B_0, символ x_1 – символом y_1 из алфавита B_1 и т.д., символ x_{r-1} заменяется символом y_{r-1} из алфавита B_{r-1}, символ x_r заменяется символом y_r снова из алфавита B_0 и т.д.

Чтобы получить достаточно сложный шифр, выберем, например, число алфавитов равным 7. Далее закодированная метка представляется в бинарной форме и заносится в изображение. Для добавления шумов в кодируемом сообщении его можно разбить на части по 2 символа, и между каждыми двумя символами кодировать дополнительные случайные 2 символа.

Таким образом, извлечение и замена метки будут значительно затруднены. Чтобы проверить, не используются ли данные нелегально, необходимо программным продуктом извлечь из изображения сокрытую информацию и сравнить ее с информацией в полях, доступных для редактирования.

Процесс внедрения метки имеет смысл осуществлять непосредственно в момент создания фотографии, т.е. в самой фотокамере. Предлагается встраивать данный алгоритм в программное обеспечение, установленное в фотокамере. Дальнейшее развитие описанной в настоящей работе идеи также возможно, причем это особенно актуально для фотоснимков формата raw.

Список цитированных источников

1. ISO/IEC IS 10918–1 | ITU–T Recommendation T. 81. JPEG standart, first edition; ins. 15.02.1994 – International Standard Organization, 1994. – 5 p.

2. Huffman, D. A Method for the Construction of Minimum-Redundancy Codes / D. Huffman // Proceedings of IRE, 1952. – Vol. 40, № 9. – P. 1098-1101.

3. Аграновский, А. В. Основы стеганографии / А.В. Аграновский [и др.]. – Ростов-на-Дону, 2003. – 116 с.

4. Романец, Ю.В. Защита информации в компьютерных системах и сетях / Ю.В.Романец, П.А. Тимофеев, В.Ф. Шаньгин. – М.: Радио и связь, 2001.– 376 с.

УДК 631.3

РАЗРАБОТКА КОНЦЕПЦИИ АРМ ДЛЯ ИССЛЕДОВАНИЯ ДЕЯТЕЛЬНОСТИ ПРЕДПРИЯТИЯ ПО ПЕРЕВОЗКЕ ГРУЗОВ

Садко В.И., Слюсарева М.А.

УО «Брестский государственный технический университет», г. Брест

Научный руководитель – Хвещук В.И., к.т.н., доцент

Общие положения. Деятельность предприятия по перевозке грузов включает решение таких производственных задач, как поиск, оценка и прием заказов, планирование и управление выполнением заказов и другие. Одной из важных задач в этой деятельности является оценка деятельности предприятия в общем и отдельных его компонентов, которая относится к задачам стратегического уровня и ориентирована на руководство предприятия. Анализ внешней среды представляет собой оценку состояния и перспектив развития важнейших, с точки зрения организации, субъектов и факторов окружающей среды – отрасли, рынков, потребителей, поставщиков и совокупности глобальных факторов внешней среды, на которые организация не может оказывать непосредственное влияние. Рассматриваются вопросы формализации данной задачи и результаты разработки концепции автоматизированного рабочего места (АРМ) для оценки деятельности предприятия.

Деятельность предприятия ориентирована на оказание услуг по перевозке грузов другим предприятиям и осуществляется в рыночных условиях. Клиентами (заказчики перевозок и потребители грузов) предприятия могут быть как юридические, так и физические лица. Отдельный груз рассматривается как неделимый и перевозится в отдельном прицепе. Груз имеет координаты погрузки и разгрузки, расстояние перевозки, стоимость перевозки. Поступление заказов на перевозку грузов для предприятия носит динамический характер и не зависит от предприятия. Перевозки осуществляются водителями предприятия на автомобилях с прицепами, которые могут быть как личными, так и в собственности предприятия. Распределение заказов на перевозку грузов между водителями, а также управление перевозками динамически осуществляют сотрудники предприятия (менеджеры и диспетчера).