Следует также иметь в виду, что информационное общество и электронное правительство – это не только абсолютно новый уровень коммуникаций, проблема состоит еще и в том, что внедрение информационных технологий требует смены ментальности – и рядовых граждан, и чиновников.

Основное внимание в ближайшей перспективе необходимо уделять вопросу дальнейшего увеличения объема государственных электронных услуг, поскольку повышение уровня информатизации в сфере работы с гражданами и организациями является одним из основополагающих принципов при дебюрократизации государственного аппарата.

УДК 004

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ДЛЯ СОКРЫТИЯ ИНФОРМАЦИИ В ЦИФРОВЫХ ИЗОБРАЖЕНИЯХ С ПОМОЩЬЮ СТЕГАНОГРАФИЧЕСКОГО МЕТОДА КОХА И ЖАО

Ражков А.Ф.
Могилевский государственный университет имени А.А. Кулешова
e-mail: razhkov.a@mail.ru

Abstract. *The problem of steganography on graphic files was considered and the following results were obtained. In the course of this work, an analysis of the subject area was carried out and the existing analogues of the software being developed were reviewed. An INFINPIC application has been developed for steganographic data hiding in image files of BMP and PNG formats using the method of relative replacement of the values of the coefficients of the discrete-cosine transform.*

В Интернете сейчас существует множество сайтов, на которых люди делятся своими фотографиями. Эти фотографии очень разнообразны: порой они очень личные, эмоциональные. Порой они причудливы и смешны, порой отображают какие-либо интересные места, интересных людей. С помощью фотографий мы обмениваемся с другими людьми своими впечатлениями о том, что мы переживаем.

А с помощью стеганографии, с виду неприметное изображение может хранить не только графическую информацию. Для чего это может быть полезно? Кодирование будет производиться с помощью метода скрытия в частотной области изображения. Стоит отметить, что размер и качество изображения, при встраивании в него информации, остается практически неизменным. Следовательно, можно хранить в открытом доступе или передавать по открытым каналам связи почти любую конфиденциальную информацию [1].

Один из наиболее распространенных на сегодня методов скрытия конфиденциальной информации в частотной области изображения заключается в относительной замене величин коэффициентов ДКП. На начальном этапе первичное изображение разбивается на блоки размерностью 8×8 пикселей. ДКП применяется к каждому блоку, в результате чего получают матрицы 8×8 коэффициентов ДКП, которые зачастую обозначают $\Omega b\,(\upsilon, \nu)$, где b – номер блока контейнера C, а (υ, ν)– позиция коэффициента в этом блоке. Каждый блок при этом предназначен для скрытия одного бита данных. Во время организации секретного канала абоненты должны предварительно договориться о двух конкретных коэффициентах ДКП из каждого блока, которые будут использоваться для скрытия данных [2].

Разработанное приложение INFINPIC позволяет встраивать информацию в изображения в форматах BMP, PNG и извлекать её, скрыв при этом сам факт внедрения. Используется метод относительной замены величин коэффициентов дискретно-косинусного преобразования (ДКП) (метод Коха и Жао), достоинством которого является устойчивость к большинству известных стеганоатак, в том числе к атаке сжатием, к аффинным преобразованиям и геометрическим атакам, а недостаток низкой пропускной способности метода

было решено исправить путем выбора на начальном этапе размерности блоков (осуществим разбиение изображения не только 8×8 пикселей, но и 4×4, 2×2).

Приложение обладает следующим функционалом:

1. Поддержание BMP, PNG форматов графических файлов.
2. Определение объёма контейнера.
3. Стеганографическое сокрытие данных в графических файлах форматов BMP, PNG методом относительной замены величин коэффициентов дискретно-косинусного преобразования.
4. Извлечение скрытых данных из графических файлов форматов BMP, PNG.
5. Сравнение двух изображений с последующим выводом результата попиксельного сравнения.
6. «Очистка изображения» осуществляется путём сокрытия случайных данных в графические файлы, благодаря чему данные, возможно имеющиеся в графических файлах, повреждаются.

На рисунке 1 представлен интерфейс приложения.

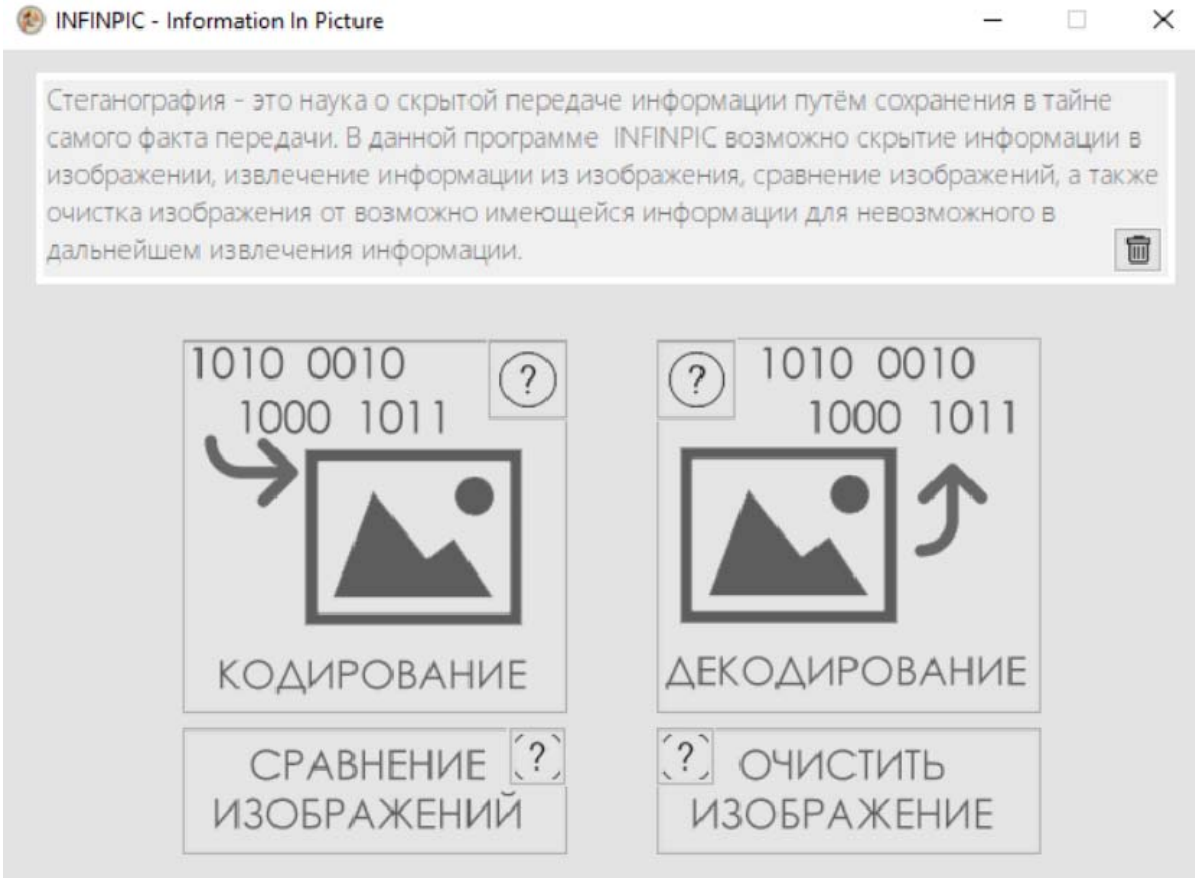

Рисунок 1 – Интерфейс приложения

Приложение отвечает всем требованиям, предъявляемым к стеганографическому программному обеспечению, и может использоваться для сокрытия данных в графических файлах форматов BMP, PNG.

После завершения разработки было проведено тестирование программного средства на ряде фотографий. Результаты тестирования на скрытность встраивания и полезный объем байтов для встраивания являются хорошими.

Список использованных источников

1. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. – К.: МК-Пресс, 2006. – С. 9-13.

2. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. – К.: МК-Пресс, 2006. – С. 130-135.

УДК 004

РАЗРАБОТКА МОБИЛЬНОГО ПРИЛОЖЕНИЯ SPOILER APP ДЛЯ СМАРТФОНОВ ПОД УПРАВЛЕНИЕМ ОПЕРАЦИОННОЙ СИСТЕМЫ ANDROID С ИСПОЛЬЗОВАНИЕМ СЕРВИСОВ GOOGLE

Ражков А.Ф., Юхновский В.В., Васильчиков И.Д.
Могилевский государственный университет имени А.А. Кулешова
e-mail: razhkov.a@mail.ru

Abstract. *Developed mobile application Spoiler App. Provides an overview of the used Google services when developing a mobile application. Created a database of spoilers of various creative works. The prospects for implementation in daily life and educational process are discussed.*

В современном мире медиапространство развивается очень быстро. Каждый день выходят новые книги, фильмы, сериалы, игры. И для того, чтобы всегда быть в курсе того, чем закончилось то или иное творческое произведение (книга, фильм, сериал, игра), было разработано приложение Spoiler App, в котором пользователю предоставляется возможность получить случайный спойлер по выбранной категории. Спойлер – информация, раскрывающая сюжетные подробности какого-либо художественного произведения. Нередко после прочитанного спойлера дальнейшее знакомство с произведением становится бессмысленным и скучным занятием.

Но также нередко бывают такие ситуации, в которых человек хочет посмотреть фильм, сериал, прочитать книгу, пройти игру, которые являются сиквелами. Сиквел – книга, фильм или любое другое творческое повествование, по сюжету являющееся продолжением какого-либо произведения. Современные франшизы фильмов, например, насчитывают около 10 частей. Для того, чтобы хорошо ориентироваться в них, либо освежить память перед новой частью, разработано приложение Spoiler App, с которым можно ознакомиться и скачать в Google Play Store: https://play.google.com/store/apps/details?id=vlad.com.spoilerapp [1].

Современные тенденции в мобильных технологиях все больше ориентируются на облачные сервисы и платформы. Например, активно развиваются сервисы Google Firebase, Amazon AWS, Microsoft Azure и другие, включающая сервисы облачной базы данных, уведомлений, хранения статических и динамических данных, аналитики и др. и позволяющие упростить создание и развертывание полнофункциональных систем с минимальным использованием собственного backend-а.

При разработке мобильного приложения активно использовались сервисы Firebase для хранения данных, работы с базой данных, контроля сбоев и аналитики.

Сервис Firebase Database использовался как онлайн-хранилище динамических данных: данные о названии книг, фильмов, сериалов, игр, ссылок на изображения обложек книг, постеров фильмов, сериалов, игр. Изначально не стояла задача сделать статическое приложение, т.к. прогнозируется необходимость вносить изменения в программу. Все мобильные приложения синхронизировали локальное хранилище данных с облачным и в каждый момент времени имели актуальные данные [2].

Также в разработке использовался сервис Firebase Storage, который предоставляет облачное пространство для хранения статических файлов: изображения, документы и др. Сервис используется для хранения изображений обложек книг, постеров фильмов,