

СЕКЦИЯ «ИНТЕЛЛЕКТУАЛЬНЫЕ ТЕХНОЛОГИИ И СИСТЕМЫ»

ОЦЕНКА СТЕГАНОГРАФИЧЕСКОЙ ЁМКОСТИ ИЗОБРАЖЕНИЙ RGB ФОРМАТА

К. В. Автушко, В. С. Садов

Белорусский государственный университет, Минск, Беларусь

E-mail: kirill.avtushko@yandex.ru

На сегодняшний день задача поиска оптимальных контейнеров в цифровой стеганографии является полностью не решенной. В работе рассмотрены блоки изображений различной тематики. Исследовано влияние корректировки цветовых компонент взятых изображений на стеганографическую ёмкость, а также выработаны конкретные рекомендации к контейнерам для увеличения стеганографической ёмкости.

Ключевые слова: стеганографическая ёмкость; изображения; RGB; стеганография; PSNR; субдискретизация.

Активное развитие цифровых технологий, систем передачи мультимедийной информации, возрастание мирового сетевого трафика обуславливает актуальность цифровой стеганографии в системах скрытой передачи информации [1].

Основные понятия стеганографической модели [2]:

- Стеганографическая система – объединение методов и средств, используемых при создании скрытого канала передачи информации по открытым информационным каналам.
- Сообщение – общее название передаваемой скрытно информации.
- Контейнер – любая информация, используемая для сокрытия тайного сообщения. Пустой контейнер не содержит секретного сообщения. Заполненный контейнер или стегоконтейнер содержит секретное сообщение.
- Стегоключ – секретный ключ, который необходим для сокрытия стегоконтейнера.

На сегодняшний день задача поиска оптимальных контейнеров и методов встраивания полностью не решена. Немалый вклад в развитие стеганографии внесли ученые Японии, Швейцарии, Англии, Соединенных Штатов Америки, Украины, России и Беларуси [1]. Поэтому в данной работе проведены исследования ёмкости таких стегоконтейнеров, как RGB изображения различных тематик (рис. 1), а именно: класс изображений «Портрет», состоящий из 100 фотографий; класс изображений «Пейзаж», состоящий из 50 фотографий; класс изображений «Картогра-

фические материалы» (Далее «Карты»), состоящий из 50 снимков со спутника.

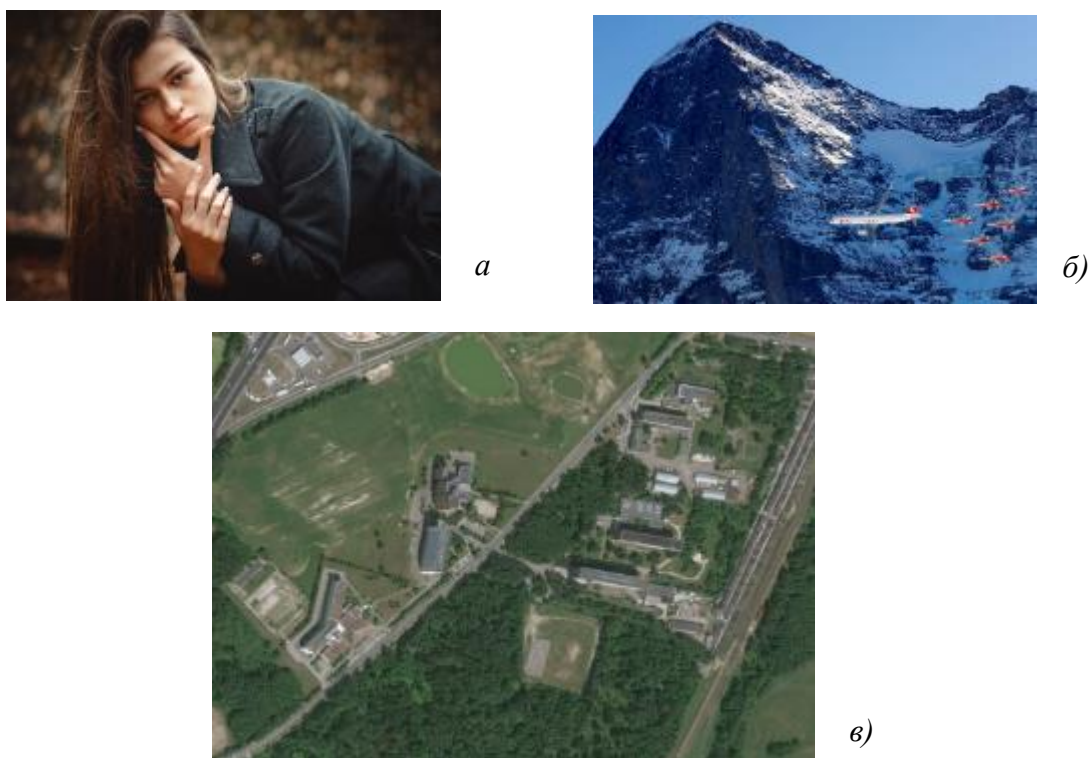


Рис. 1. Примеры различных классов изображений, используемых в работе: класс «Портрет»- (а), класс «Пейзаж»- (б), класс «Картографические материалы»- (в)

Для «чистоты» результатов в классе «Портрет» были взяты фотографии, предоставленные белорусским писателем, поэтом, драматургом, фотографом Игорем Сидоруком, а не изображения из сети Интернет. Для наполнения класса «Пейзаж» использовались снимки с телеканала «Моя планета» из раздела «Фото дня». Картографические материалы были взяты из открытого сервиса «Яндекс. Карты»

В компьютерных системах цифровые изображения, как правило, подвергаются сжатию для уменьшения размера описания, например, в формате JPEG [3-5]. Рассмотрены следующие виды субдискретизации (предварительное сжатие) [6] наших контейнеров из вышеперечисленных классов: 1:2 по горизонтали изображений при усреднении в каждой из трех цветовых компонент, 1:2 по горизонтали при усреднении синей и красной компонент изображения, 1:2 по горизонтали при усреднении в зеленой и красной компонентах, 1:2 по горизонтали при усреднении синей и зеленой компонент. Аналогичные действия проводились по вертикали изображений при усреднении 1:2, а также 1:4. В сумме нами рассмотрено 12 видов снижения цветового разрешения. Исследования проводились в рабочей среде MATLAB. В качестве критерия оценки при-

годности исследуемого метода использовано пиковое отношение сигнала к шуму (PSNR) [7], а также изображения оценивались визуально. В работе [8] показано, что искажения в изображении не заметны визуально, когда PSNR имеет значение не ниже 40 дБ [8].

В ходе работы установлено, что наилучшие показатели PSNR достигаются в изображениях типа «Портрет», где 17% изображений из рассмотренной выборки имеют показатели пикового отношения сигнала к шуму в интервале 43-50 дБ. Выявлено, что для оптимальных, с точки зрения стеганографии, показателей PSNR портреты должны быть однородны по яркости. Это достигается размытием заднего плана изображения. Далее в таблице и на рис. 2 представлены средние значения PSNR для всех рассмотренных тематик фотографий по всем видам усреднения.

Таблица

Средние значения PSNR для рассмотренных тематик изображений

Тип изображения	«Портреты»	«Карты»	«Пейзажи»
PSNR	40,6 дБ	38,2 дБ	35,6 дБ

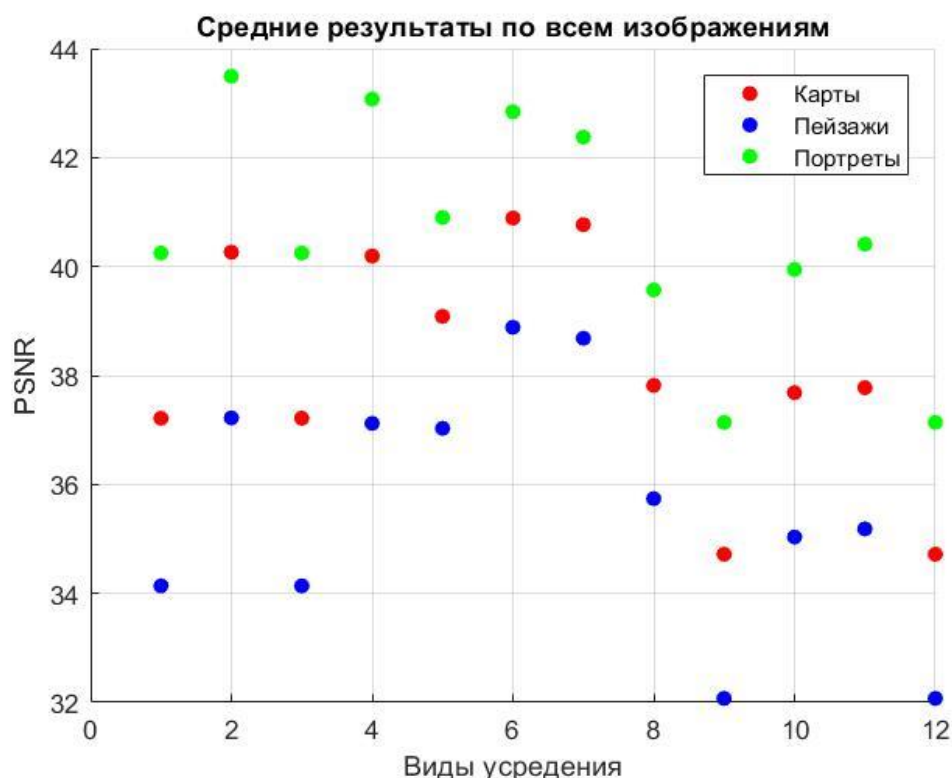


Рис. 2. Усредненные результаты субдискретизации трех различных тематик изображений.

По полученным результатам видно, что «Пейзажи» имеют наихудшие показатели зашумленности (стойкости) контейнеров к встраиванию информации.

Стоит отметить, что для «Портретов» наилучшим является второй метод субдискретизации, а для «Пейзажей» и «Карт» - шестой. Это соответствует методам субдискретизации 1:2 по вертикали с сохранением красного канала и 1:2 по горизонтали с сохранением красного канала. При рассмотрении значений PSNR во всех 12 взятых видах усреднения яркости цветовых компонент, можно заметить, что наилучшие средние численные значения имеют те виды, где усреднение происходит в синем и зеленом канале с сохранением красной цветовой компоненты. Для «Портретов» это:

1:2 по вертикали – среднее значение: 43,5 дБ;

1:2 по горизонтали – среднее значение: 42,8 дБ;

1:4 – среднее значение: 40,4 дБ.

При визуальной оценке качества субдискретизации результаты совпадают с оценкой по PSNR (рис. 3).



а)



б)



в)



г)

Рис. 3. Исходное изображение - (а); фрагмент исходного изображения с увеличением 75% - (б); фрагмент изображения после субдискретизации (1:4 с усреднением в каждом канале) с увеличением 75% и PSNR 41дБ - (в); фрагмент изображения после субдискретизации (1:2 по вертикали с сохранением красного канала) с увеличением 75% и PSNR 48 дБ - (г)

БИБЛИОГРАФИЧЕСКИЕ ССЫЛКИ

1. Садов В. С. Компьютерная стеганография: конспект лекций. Минск: БГУ. 2010. 232 с.

2. Аграновский А. В. и др. Основы компьютерной стеганографии: учебное пособие для вузов. Москва: Радио и связь. 2003. 152 с.
3. Быков С. Ф. Алгоритм сжатия JPEG с позиции компьютерной стеганографии // Защита информации. Конфидент. 2000. №3. С. 26–33.
4. Миано Дж. Форматы и алгоритмы сжатия изображений в действии: учебное пособие. Москва: Триумф. 2003. 336 с.
5. Tinsley R. Steganography and JPEG Compression: Final Year Project Report. University of Warwick, UK, 1996. 114p.
6. Цветовая субдискретизация понятным языком – немного отдаем, чтобы много выиграть [Электронный ресурс]. – Режим доступа: <http://projectorworld.ru/blog/957.html>. – Дата доступа: 11.12.2019.
7. Пиковое отношение сигнала к шуму [Электронный ресурс]. – Режим доступа: <https://ru.wikipedia.org/?oldid=102495551>. – Дата доступа: 02.10.2019.
8. Чваркова И. Л. Повышение пропускной способности и стойкости стеганографических систем: диссертация на соискание степени кандидата технических наук // Минск. 2008.

СТРУКТУРА МЕТОДИКИ МОДЕЛИРОВАНИЯ УГРОЗ КОМПЬЮТЕРНЫХ СИСТЕМ НА ОСНОВЕ ПРЕДМЕТНО- ОРИЕНТИРОВАННЫХ МОДЕЛЕЙ

А. И. Бражук

*ГрГУ им. Я. Купалы, г. Гродно, Республика Беларусь
E-mail: brazhuk@grsu.by*

Предложена методика моделирования угроз компьютерных систем на основе предметно-ориентированных моделей угроз, которая позволяет автоматически формировать списки релевантных угроз и контрмер на основе описаний архитектур компьютерных систем (диаграмм потоков данных). Методика использует язык онтологий OWL и функции автоматического логического вывода. В отличие от существующих решений методика позволяет внедрить объектно-ориентированный подход, обеспечить интеграцию с источниками связанных открытых данных и представлять контрмеры как контекстные шаблоны безопасности.

Ключевые слова: моделирование угроз; онтология; OWL.

Введение. Моделирование угроз компьютерных систем с использованием диаграмм потоков данных (DFD - Data Flow Diagram) было предложено некоммерческой организацией OWASP (Open Web Application Security Project) и корпорацией Microsoft. Для декомпозиции структуры приложения и описания потоков данных, команда разработчиков применяет простое визуальное представление архитектуры приложения посредством диаграмм DFD; на последующих стадиях полученные диаграммы используются для построения неформальной модели угроз (перечня угроз и противодействий этим угрозам) путем дискуссий с приме-