ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
СПбГУТ))) Март 2016 Том 4 № 1 ISSN 2307-1303 http://www.itt.sut.ru
TELECOM IT
March 2016 Vol. 4 Iss. 1 ISSN 2307-1303 http://www.itt.sut.ru

О ПРИМЕНИМОСТИ СТЕГАНОГРАФИЧЕСКИХ СИСТЕМ ДЛЯ «ИНТЕРНЕТА ВЕЩЕЙ»

М. А. Клюев[1], Т. А. Минаева[1], А. Я. Омётов[2]

[1] Санкт-Петербургский государственный университет аэрокосмического приборостроения, Санкт-Петербург, 190000, Российская Федерация
[2] СПбГУТ, Санкт-Петербург, 193232, Российская Федерация
Адрес для переписки: alexander.ometov@gmail.com

Информация о статье
УДК 621.391
Язык статьи – русский.
Поступила в редакцию 21.01.16, принята к печати 22.02.16.

Ссылка для цитирования: Клюев М. А., Минаева Т. А., Омётов А. Я. О применимости стеганографических систем для «Интернета Вещей» // Информационные технологии и телекоммуникации. 2016. Том 4. № 1. С. 104–114.

Аннотация
В современных беспроводных сетях связи все чаще фигурирует термин Интернет Вещей (IoT) проникая во многие области жизни обычных людей. Сообщество исследователей в сферах телекоммуникаций и информационной безопасности обеспокоено, что IoT может стать огромной угрозой современному обществу с точки зрения конфиденциальности, таким образом, обозначая важное направление исследований. Авторы работы предлагают потенциальное повешение качества конфиденциальности IoT за счет использования методов стегоанализа для сокрытия информации в передаваемых данных. В данной работе рассмотрены основные задачи и классификация стегосистем и методов их анализа, приведены результаты практической реализации некоторых методов статистического стеганоанализа, а также определена применимость в контексте Интернета Вещей.
Ключевые слова
стеганоанализ, Интернет Вещей, обработка изображений.

SECURING DATA WITH STEGANOGRAPHY FOR INTERNET OF THINGS

M. Klyuev[1], T. Minaeva[1], A. Ometov[2]

[1] Saint-Petersburg state University of Aerospace Instrumentation, St. Petersburg, 190000, Russian Federation
[2] SPbSUT, St. Petersburg, 193232, Russian Federation
Corresponding author: alexander.ometov@gmail.com

Article info
Article in Russian.
Received 21.01.16, accepted 22.02.16.

For citation: Klyuev M., Minaeva T., Ometov A.: Securing Data with Steganography for Internet of Things // Telecom IT. 2016. Vol. 4. N 1. pp. 104–114 (in Russian).

Abstract
In this paper, authors consider cases related to the confidentiality question of the Internet of Things (IoT). As a matter of fact, both Information Security and Telecommunications communities are concerned about what information may leak out via IoT. Therefore, the need of a secure environment is vital securing the data transmission over the wireless medium. In this work, authors survey the main steganography systems and the corresponding methods of their analysis, followed by practical implementation of the statistical ones.

Keywords
Steganography, Internet of Things, Image steganography.

Введение

Все больше внимания у исследователей беспроводных технологий вызывает концепция Интернета Вещей (IoT), объединяющая в себе множество разнообразных электронных устройств, технологий связи и протоколов взаимодействия [1]. Гиганты индустрии, подобные CISCO, предсказывают наличие более 50 миллиардов активных устройств уже к 2020 году [2]. Повышение мощностей и одновременное удешевление устройств производит дополнительную стимуляцию повсеместной интеграции Интернета Вещей. В то же время, многие пользователи с сомнением относятся к потенциальному использованию умных устройств в своих домах и на предприятиях. Пусть простота использования и видится привлекательной, проблемы информационной безопасности IoT уже попали в пятерку критических вопросов в 2015 году [3].

Главным вопросом безопасности автономных умных устройств можно считать раскрытие информации третьей стороне [4]. В особенности это касается узлов с низким уровнем защищенности и невысокой вычислительной мощностью, такие как, например, умные телевизоры, IP камеры, умные няни и прочие [5]. В то же время огромное влияние оказывает неоднородность сетей с точки зрения протоколов и беспроводных технологий, что влечет за собой еще большие проблемы конфиденциальности.

В данной работе авторы выдвигают потенциальное решение по повышению конфиденциальности IoT сетей на основании классических методов стеганографии. Данная статья имеет следующую структуру: во втором разделе дается вводная информация по стегоанализу изображений. Далее, приводится оценка эффективности рассмотренных методов посредством имитационного моделирования. Последний раздел подводит итоги рассуждений.

Стеганоанализ изображений

Стеганографическая система (далее – стегосистема) представляет собой набор различных методов и средств, используемых для создания скрытого канала передачи информации [6]. К основным задачам, которые решаются стегосистемами, можно отнести: защиту авторских прав на некоторые виды интеллектуальной собственности; защиту конфиденциальной информации от несанк-

ционированного доступа; преодоление системы мониторинга и управления сетевыми ресурсами; камуфлирование программного обеспечения. По уровню обеспечения стойкости к пассивным атакам стегосистемы можно разделить на теоретически стойкие, практически стойкие и нестойкие [7].

Теоретически стойкие стегосистемы осуществляют сокрытие информации в тех элементах контейнера, значения которых не превышают уровня шума или погрешности квантования [8]. Невозможность различения пустых и заполненных контейнеров таких систем должны быть теоретически доказуемы [9]. Под контейнером для скрытия информации понимается любой файл, структура и размер которого позволяют скрыть необходимые данные. Возможность выявления стеганоконтейнеров, созданных практическими стойкими стегосистемами, не исключена, но на данный момент противник не располагает необходимыми для этого ресурсами.

Стегосистема является нестойкой, если имеются методы, которые позволяют выявить факт эксплуатации системы [10]. На данный момент самым распространенным, но, в то же время, наименее стойким к обнаружениям методом стеганографического скрытия, является метод замены наименее значимых бит (НЗБ, LSB). Идея метода заключается в замене от одного до четырех битов в байтах цветового представления точек данного изображения битами скрываемого сообщения. Такой метод применяется к растровым изображениям, которые представлены в формате без компрессии – BMP [9]. Сокрытие в JPEG-файлах выполняется аналогичным способом, однако, вместо цветовых составляющих изменяются квантованные дискретные косинусные коэффициенты.

В статье [6] предлагается следующая классификация стеганоаналитических методов:

1) в зависимости о количества информации, доступной аналитику: направленные; универсальные;

2) по критерию цели атаки: статические; динамические; вспомогательные;

3) в зависимости от объекта поиска в контейнерах: визуальные; сигнатурные; статистические.

Далее в статье рассмотрены методы третьей группы, однако, перед их рассмотрением необходимо оценить уровень шума, создаваемый встраиванием в НЗБ контейнера, которое было использовано при реализации и оценке методов статистического стеганоанализа.

Первая оценка, являющаяся абсолютной, среднеквадратичное отклонение реального сигнала, описывающего изображение, от полезного [11]:

$$Nrms = \sqrt{\frac{\sum_{i=0}^{k-1}(B_i - A_i)^2}{k}},$$

где $Nrms$ – среднеквадратичное отклонение реального сигнала, описывающего изображение, от полезного; B_i – значение i-го элемента заполненного контейнера; A_i – значение i-го элемента пустого контейнера; k – количество элементов в контейнере.

На основании абсолютной оценки может быть вычислена относительная оценка – пиковое отношение полезного сигнала к шуму PSNR (*peak-to-peak signal-to-noise ratio*) [9], измеряемое в децибелах:

$$PSNR = 20\log_{10}\left(\frac{A_{\max}}{Nrms}\right),$$

где *PSNR* – пиковое отношение полезного сигнала к шуму; A_{max} – максимальное значение сигнала; *Nrms* – среднеквадратичное отклонение реального сигнала, описывающего изображение, от полезного.

Максимальное значение сигнала в полноцветном BMP-изображении равно 255. После встраивания информации описанным выше способом значение *PSNR* не превысило 52 дБ. Типичные значения *PSNR* для сжатия изображений лежат в пределах 30–40 дБ. Так как это отношение полезного сигнала к шуму, то чем выше значение *PSNR*, тем меньше шума создает встраивание.

Методы первой группы – визуальные, основанные на особенностях зрительной системы человека, являются самыми простыми, поскольку для проведения анализа такими методами достаточно лишь посмотреть на изображение. Данный метод устанавливает ограничения на объем скрываемых данных, поскольку изменение большого числа бит может привести к слишком сильному искажению изображения, что будет сразу замечено при визуальном анализе. Однако, такой метод анализа подходит лишь для файлов формата BMP, поскольку в JPEG-информация скрывается не в самих пикселях, а в значениях квантованных дискретных косинусных коэффициентов. И, даже если изменения будут заметны, то их можно объяснить процедурой компрессии файла.

Вторая группа – сигнатурные методы, суть которых заключается в синтаксическом анализе предъявленной на вход распознающего устройства последовательности терминальных символов, определяющих контейнер. В случае обнаружения принадлежности предъявленной на вход распознавателя цепочки терминальных символов языку, описывающему ту или иную стеганосистему, принимается решение об ее использовании для скрытия информации. В качестве терминальных символов обычно берут все или часть стандартных символов ASCII – латинские буквы, цифры и специальные символы [12].

Оценка эффективности стеганографических методов

Для оценки эффективности статистических методов было реализовано приложение на языке C++, осуществляющее анализ изображений формата BMP на наличие скрытой информации тремя статистическими методами. Язык программирования выбран таким образом не случайно – представляется универсальная система, которая может быть протестирована практически на любом современном устройстве IoT независимо от его мощности. В качестве примера использовано типовое изображение airplane.bmp. Информация, представляющая собой псевдослучайный набор нулей и единиц, заносилась поочередно в последний бит каждой цветовой составляющей и проводилось сравнение стегоконтейнера с естественным.

В первую очередь мы исследовали метод анализа распределения пар значений на основе критерия Хи-квадрат приведен в статье [13] и основан на зна-

нии того, что младшие биты изображений не являются случайными и частоты двух соседних элементов контейнера должны находиться достаточно далеко от значения частоты среднего арифметического этих элементов.

В «пустом» изображении ситуация, когда частоты элементов со значениями *2N* и *2N+1* близки по значению, встречается достаточно редко. При встраивании информации данные частоты сближаются или становятся равными (рис. 1). Идея атаки хи-квадрат заключается в поиске этих близких значений и подсчете вероятности встраивания на основе того, как близко располагаются значения частот четных и нечетных элементов анализируемого контейнера к среднему пары.

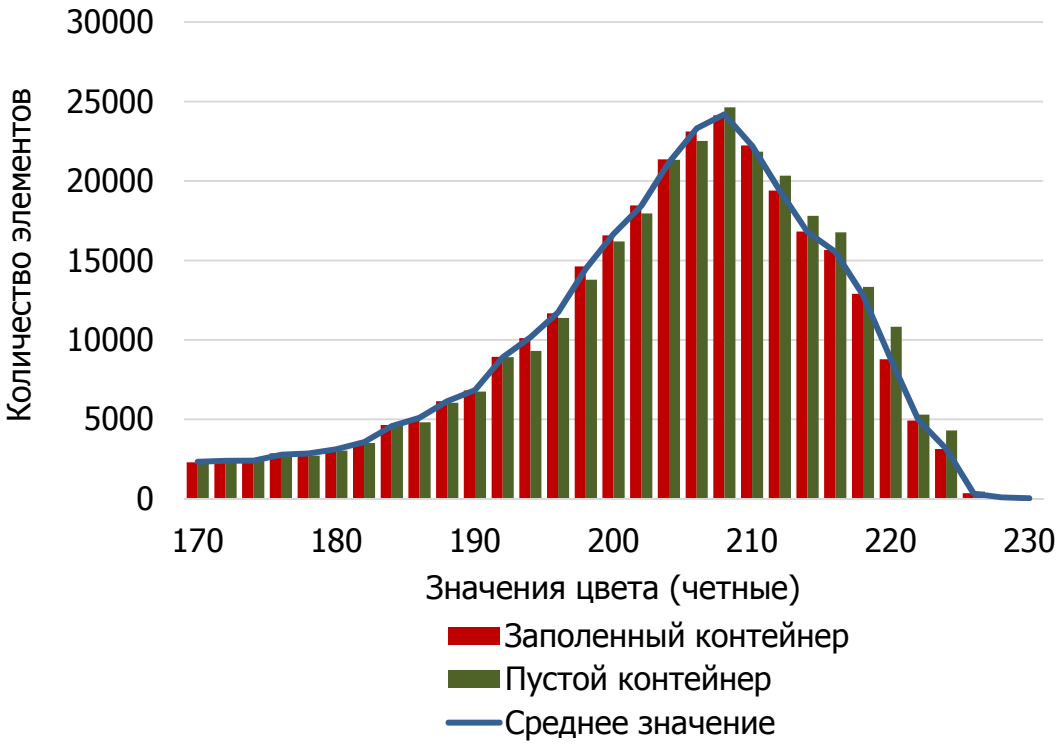

Рис. 1. Фрагмент гистограммы пустого и заполненного контейнеров изображения

Из гистограммы видно, что частоты четных элементов в парах заполненного контейнера (левые столбцы) расположен ближе к линии среднего, чем аналогичные частоты четных элементов незаполненного контейнера (правые столбцы).

Теоретически ожидаемая частота элементов пары была рассчитана по следующей формуле:

$$n_i^* = \frac{\left|\left\{\text{colour} \middle| \text{sortedIndexOf(colour)} \in \{2i, 2i+1\}\right\}\right|}{2},$$

где n_i^* – теоретически ожидаемая частота появления элементов i-й пары.

Эмпирическая частота появления четных элементов контейнера была вычислена следующим образом:

$$n_i = \left|\left\{\text{colour} \middle| \text{sortedIndexOf(colour)} = 2i\right\}\right|,$$

где n_i – эмпирическая частота появления четного элемента i-й пары.

На основании полученных значений была вычислена статистика хи-квадрат с k–1 степенью свободы:

$$\chi^2_{k-1} = \sum_{i=1}^{k} \frac{\left(n_i - n_i^*\right)^2}{n_i^*},$$

где χ^2_{k-1} – статистика хи-квадрат с k–1 степенью свободы; k – количество пар значений элементов контейнера; n_i – эмпирическая частота появления четного элемента i-й пары; n_i^* – теоретически ожидаемая частота появления элементов i-й пары.

После получения статистики хи-квадрат была вычисления вероятность встраивания информации в изображение:

$$p = 1 - \frac{1}{2^{\frac{k-1}{2}} \Gamma\left(\frac{k-1}{2}\right)} \int_0^{\chi^2_{k-1}} e^{-\frac{x}{2}} x^{\frac{k-1}{2}-1} dx,$$

где p – вероятность встраивания информации в изображение; k – количество пар значений элементов контейнера; χ^2_{k-1} – статистика хи-квадрат с k–1 степенью свободы.

Сравнение работы метода при применении к пустому контейнеру, контейнеру с полным заполнением и контейнеру, заполненному на 50 % представлено на графике (рис. 2).

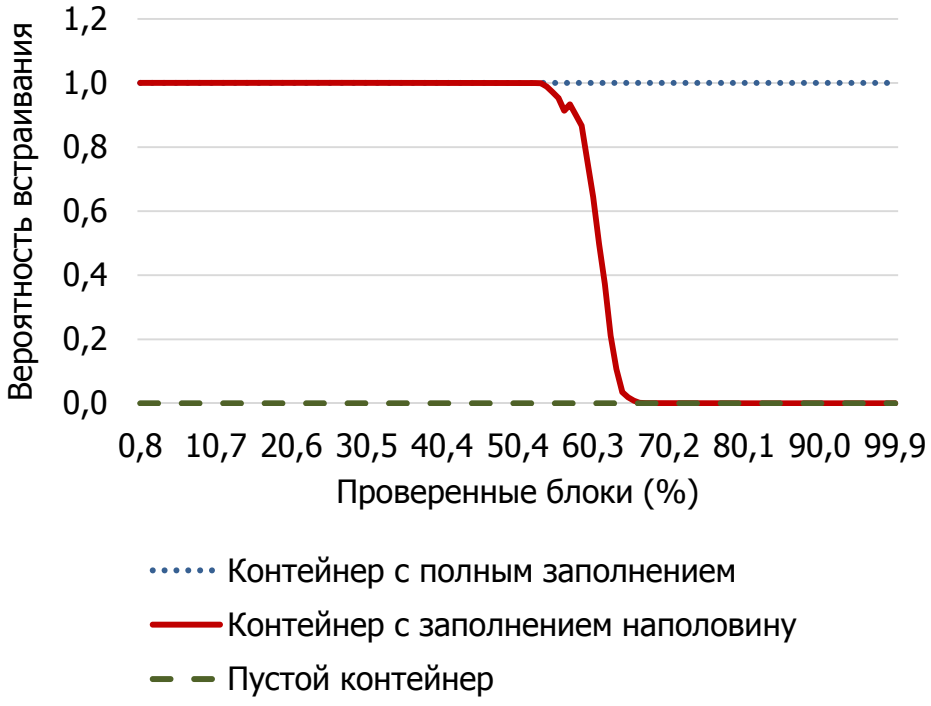

Рис. 2. График вероятность встраивания информации в изображения

Изображение размером 512 на 512 пикселей анализировалось блоками по 2000 пикселей, после каждого блока вычислялась статистика по проанализированной части изображения и вычислялась вероятность встраивания. Как видно из графика, вероятность встраивания в пустом контейнере (штрих) лежит на нулевой отметке, вероятность в заполненном контейнере (пунктир) – на единичной отметке. При заполнении контейнера на 50 % вероятность встраивания начинает убывать при проверке 53 % изображения – после того, как в статистике накопится достаточное число неизмененных элементов.

Следующий метод – метода оценки числа переходов значений младших бит в соседних элементах контейнера. Метод основывается на знании того, что между младшими битам соседних элементов контейнера имеются корреляционные связи. Зависимость битов в младших разрядах соседних элементов контейнера имеет марковский характер [14], причем параметры такой зависимости зависят от номера разряда.

Понятие «переход» подразумевает переход значения i-го элемента в значение $(i+1)$-го элемента. Так как анализируется двоичная последовательность, то возможно четыре типа переходов – из 0 в 0, из 0 в 1, из 1 в 0 и из 1 в 1. По полученным результатам строится гистограмма, где каждый столбец показывает число переходов (рис. 3).

Рис. 3. Гистограмма частот переходов младших бит в элементах контейнера

По гистограмме видно, что количество различных переходов в пустом контейнере значительно отличается, а при встраивании информации эта разница убывает. В контейнере, где заполнены все младшие биты, количество различных переходов практически равно.

Таким образом, чем больше информации встроено в изображение, тем больше шансов обнаружить такое встраивание. На практике же предположение о встраивании может быть сделано, если контейнер заполнена на 60 %

и более – в этом случает количество различных переходов уже достаточно близко к среднему числу переходов.

Последний из рассматриваемых методов – метод оценки частот появления *k*-битовых серий младших бит контейнера. Аналогично предыдущему данный метод позволяет провести оценку равномерности распределения элементов контейнера на основе частот появления серий элементов, состоящих из *k* бит.

Для естественных контейнеров, частоты появления различных серий находятся достаточно далеко от средней частоты. Как и в предыдущем методе, при встраивании информации частоты сближаются и постепенно, при увеличении объема встраиваемой информации, становятся ближе к средней частоте. Это продемонстрировано на гистограмме (рис. 4), составленной по частотам появления серий из трех бит.

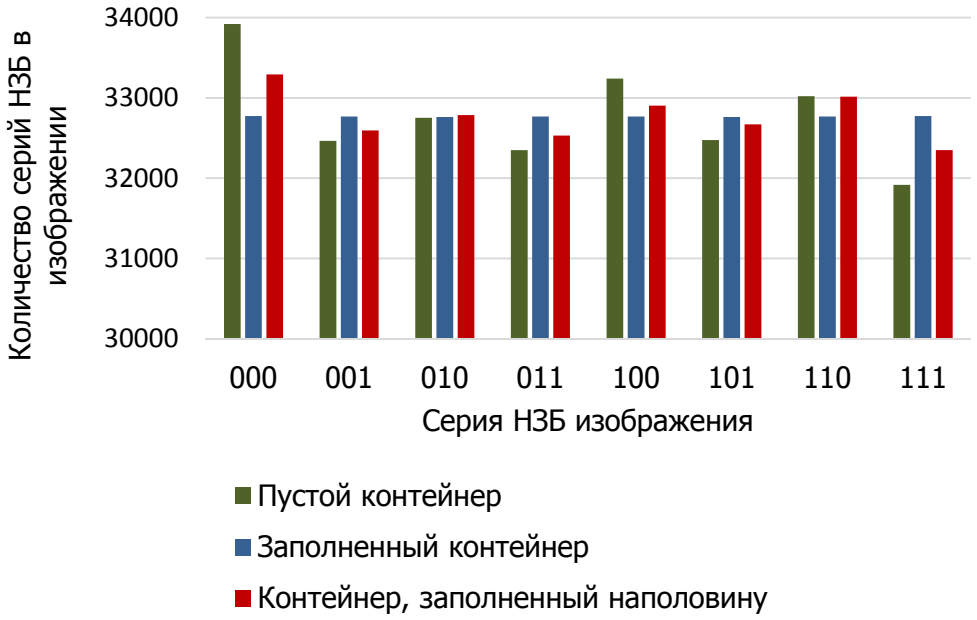

Рис. 4. Гистограмма частот появления серий из трех бит в потоке НЗБ контейнера

Видно, что результат работы метода аналогичен результату предыдущего, так как методы основываются на одних и тех же свойствах естественных контейнеров, а именно корреляционных связях между соседними элементами контейнера.

Заключение

Уже сегодня пользователи сталкиваются с проблемой конфиденциальности Интернета Вещей, что становится все более актуальным из-за его повсеместной интеграции. Как следствие, необходимость в высоком уровне защищенности данных становится одной из главных задач его развития. В данном исследовании были исследованы различные типовые изображения, потенциально передаваемые через IoT – фото людей и животных, природы и техники, спутниковые снимки и 3D-графика (рис. 5).

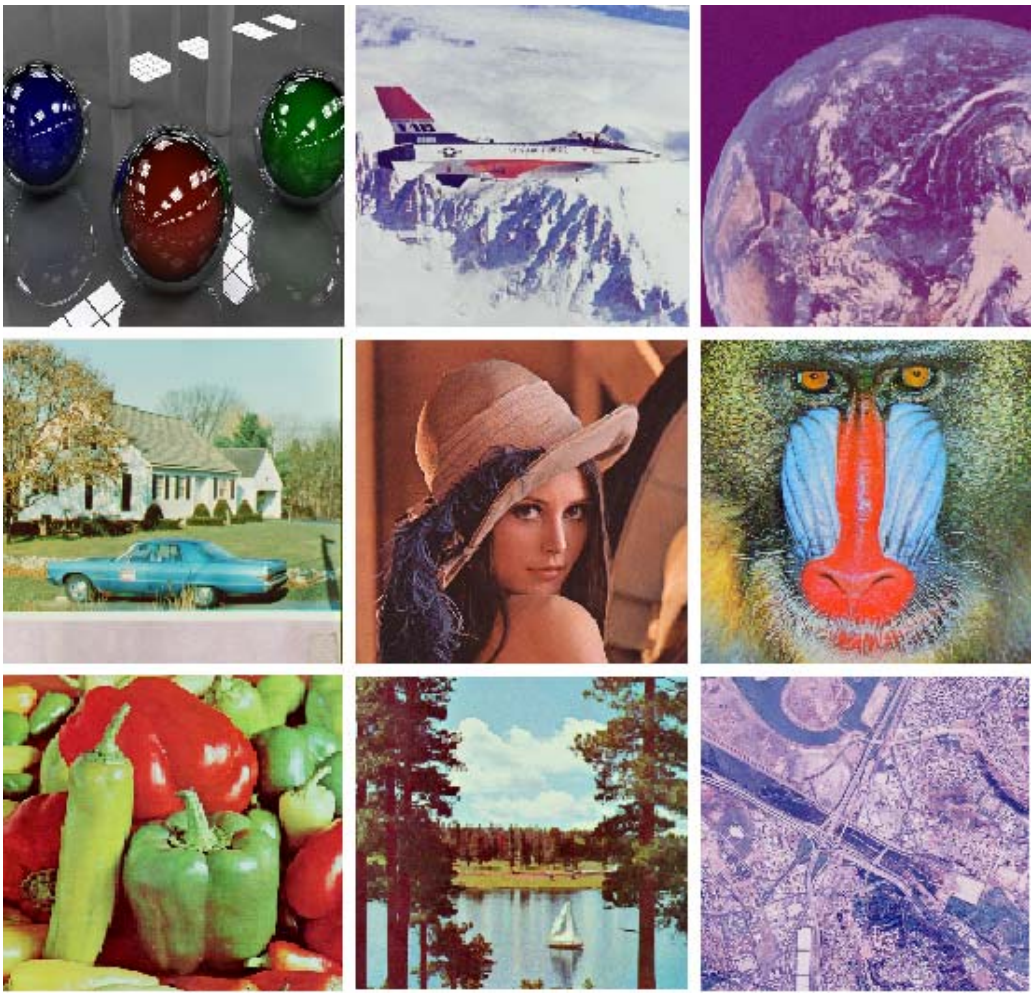

Рис. 5. Примеры тестовых изображений

На всех тестовых изображениях рассмотренные методы дают схожий результат, следовательно, данные методы применимы как к изображениям объектов реального мира, так и к изображениям, созданным при помощи компьютерной графики. Изображения, прошедшие компрессию, а затем декомпрессию, а также изображения с искусственно созданным шумом не вызвали ложного срабатывания ни одного из трех рассмотренных методов стегоанализа. В качестве обхода данного метода может быть рассмотрено использование адаптивных алгоритмов, не изменяющих распределение элементов изображения, а также наложение шума таким образом, чтобы происходило ложное срабатывание [15]. На основании вышеперечисленного показана применимость методов стегоанализа для Интернета Вещей.

Литература

1. Кучерявый А. Е. Интернет Вещей // Электросвязь. 2013. № 1. С. 21–24.
2. Osseiran A., Braun V., Hidekazu T., Marsch P., Schotten H., Tullberg H., Uusitalo M. A., Schellman M. The foundation of the mobile and wireless communications system for 2020 and beyond: Challenges, enablers and technology solutions. In IEEE 77th Vehicular Technology Conference (VTC Spring). 2013. pp. 1–5.
3. Bradley T. Experts pick the top 5 security threats for 2015. PC WORLD. 2015. pp. 1–3.
4. Atamli A. W. Threat-Based Security Analysis for the Internet of Things // International Workshop on Secure Internet of Things (SIoT). 2014. pp. 35–43.

5. Pokric B., Krco S. and Pokric M. Augmented Reality Based Smart City Services Using Secure IoT Infrastructure. In 28th International Conference on Advanced Information Networking and Applications Workshops (WAINA). 2014. pp. 803–808.

6. Генне О. В. Основные положения стеганографии // Защита информации. Конфидент. 2000. № 3. С. 20–25.

7. Кошкина Н. В. Обзор и классификация методов стеганоанализа // Управляющие системы и машины. 2015. № 3 (257). С. 3–12.

8. Коржик В. И., Небаева К. А., Алексеев С. М. Использование модели канала с шумом для построения стегосистемы // Телекоммуникации. 2013. Спецвыпуск. С. 33–36.

9. Грибунин В. Г. Цифровая стеганография. СПб. : СОЛОН-Пресс, 2002. 280 с.

10. Коржик В. И., Кочкарев А. И., Флаксман Д. А. Система цифровых водяных знаков с повторным вложением информации по различным алгоритмам // Телекоммуникации. 2014. № 7. С. 22–44.

11. Лапшенков Е. М. Неэталонная оценка уровня шума цифрового изображения на основе гармонического анализа // Компьютерная оптика. 2012. Том 36. № 3. С. 439–447.

12. Швидченко И. В. Методы стеганоанализа для графических файлов // Искусственный интеллект. 2010. № 4. С. 697–705.

13. Westfeld A., Pfitzmann A. Attacks on Steganographic Systems: Breaking the Steganographic Utilities EzStego, Jsteg, Steganos and STools-and Some Lessons Learned // 3rd International Workshop on Information Hiding. 2000.

14. Барсуков В. С., Романцов О. П. Оценка уровня скрытности мультимедийных стеганографических каналов хранения и передачи информации // Специальная Техника. 2000. № 1.

15. Коржик В. И., Курбатов Е. В. Атака на систему цифровых водяных знаков с использованием методов статистического оценивания // Вопросы защиты информации. 2005. № 2 (69). С. 14–20.

References

1. Kucheryavy A. E. The Internet of Things // Elektrosvyaz'. 2013. № 1. pp. 21–24.

2. Osseiran A., Braun V., Hidekazu T., Marsch P., Schotten H., Tullberg H., Uusitalo M. A., Schellman M. The foundation of the mobile and wireless communications system for 2020 and beyond: Challenges, enablers and technology solutions. In IEEE 77th Vehicular Technology Conference (VTC Spring). 2013. pp. 1–5.

3. Bradley T. Experts pick the top 5 security threats for 2015. PC WORLD. 2015. pp. 1–3.

4. Atamli A. W. Threat-Based Security Analysis for the Internet of Things // International Workshop on Secure Internet of Things (SIoT). 2014. pp. 35–43.

5. Pokric B., Krco S. and Pokric M. Augmented Reality Based Smart City Services Using Secure IoT Infrastructure. In 28th International Conference on Advanced Information Networking and Applications Workshops (WAINA). 2014. pp. 803–808.

6. Genne O. V. The Main Provisions of Steganography // Journal "Information Security. Confident". 2000. № 3. pp. 20–25.

7. Koshkina N. V. Review and Classification of Steganography Methods// Control Systems and Machines (or Computers). 2015. № 3 (257). pp. 3–12.

8. Korzhik V. I., Nebaeva K. A., Alekseev S. M. Using the Noisy Channel Model for Building a Stegosystem // Telecommunications. 2013. Special Issue. pp. 33–36.

9. Gribunin V. G. Digital Steganography. SPb: SOLON-Press, 2002. 280 p.

10. Korzhik V. I., Kochkarev A. I., Flaksman D. A. The System of Digital Watermarks with Reembedding Information by Different Algorithms // Telecommunications. 2014. № 7. pp. 22–44.

11. Lapshenkov E. M. Non-reference Evaluation of Digital Image Noise Level Based on Harmonic Analysis // Computer Optics. 2012. Vol. 36. № 3. pp. 439–447.

12. Shvidchenko I. V. Steganalysis Methods for Image Files // Artificial Intelligence. 2010. № 4. pp. 697–705.

13. Westfeld A., Pfitzmann A. Attacks on Steganographic Systems: Breaking the Steganographic Utilities EzStego, Jsteg, Steganos and STools-and Some Lessons Learned // 3rd International Workshop on Information Hiding. 2000.

14. Barsukov V. S., Romantsov O. P. Estimate of Level Secrecy for Steganographic Media Storage and Transmission Channel // Special Equipment. 2000. № 1.

15. Korzhik V. I., Kurbatov E. V. Attack on the System Digital Watermarks with Using Methods of Statistical Estimation // Information Security Questions. 2005. № 2 (69). pp. 14–20.

Клюев Максим Андреевич – студент, Санкт-Петербургский государственный университет аэрокосмического приборостроения, Санкт-Петербург, 190000, Российская Федерация, kluevsky@gmail.com

Минаева Тамара Александровна – студентка, Санкт-Петербургский государственный университет аэрокосмического приборостроения, Санкт-Петербург, 190000, Российская Федерация, minaeva-toma-ya@yandex.ru

Омётов Александр Ярославич – аспирант, СПбГУТ, Санкт-Петербург, 193232, Российская Федерация, alexander.ometov@gmail.com

Klyuev Maksim – student, Saint-Petersburg University of Aerospace Instrumentation, St. Petersburg, 190000, Russian Federation, kluevsky@gmail.com

Minaeva Tamara – student, Saint-Petersburg University of Aerospace Instrumentation, St. Petersburg, 190000, Russian Federation, minaeva-toma-ya@yandex.ru

Ometov Aleksandr – postgraduate, SPbSUT, St. Petersburg, 193232, Russian Federation, alexander.ometov@gmail.com