последний слой шифрования. Отправитель остается анонимным, потому что каждый промежуточный узел знает только о местоположение непосредственно предшествующих и следующих узлов сети.

Таким образом, использование современных технологий дает возможность организации Mesh-сети, в которой предусмотрены вопросы безопасности. Такая сеть обеспечивает безопасность передаваемых данных, анонимность узлов Mesh-сети, а также невозможность проведения атак типа «человек по середине» из-за своей распределенной структуры.

Литература

1. A Security Analysis of the 802.11s Wireless Mesh Network Routing Protocol and Its Secure Routing Protocols [Электронный ресурс]. – Режим доступа: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3821297, свободный (дата обращения: 19.03.2018).

2. Wi-Fi Direct [Электронный ресурс]. – Режим доступа: https://www.wi-fi.org/discover-wi-fi/wi-fi-direct, свободный (дата обращения: 10.03.2018).

3. Multipeer Connectivity Framework [Электронный ресурс]. – Режим доступа: https://developer.apple.com/documentation/multipeerconnectivity, свободный (дата обращения: 15.03.2018).

4. Mesh-сети стандарта IEEE 802.11s: протоколы маршрутизации / В.М. Вишневский, Н.Н. Гузаков, Д.В. Лаконцев // Журнал «Первая миля». – 2009. – № 1. С. 16–21.

5. Zapata M.G., Mobile Ad Hoc Networking Working Group INTERNET DRAFT Secure Ad Hoc On-Demand Distance Vector (SAODV) [Электронный ресурс]. – Режим доступа: http://people.ac.upc.edu/guerrero/papers/draft-guerrero-manet-saodv-06.txt, свободный (дата обращения: 15.03.2018).

Т.Е. Андросова, В.А. Федосеев

МЕТОД ВСТРАИВАНИЯ ИНФОРМАЦИИ В ИЗОБРАЖЕНИЯ В ФОРМАТЕ JPEG 2000

(Самарский университет)

Формат сжатия изображений JPEG 2000, несмотря на меньшую в сравнении с JPEG популярность у пользователей, позволяет обеспечивать лучшее сжатие и потому широко применяется, в частности, в системах дистанционного зондирования, медицинской визуализации и ряде других областей [1]. Это обусловливает актуальность задачи защиты изображений в формате JPEG 2000 от несанкционированных изменений. Так, например, получателю данных дистанционного зондирования необходимо иметь уверенность в отсутствии их фальсификаций, а доктор, ставящий диагноз на основании цифрового снимка, должен быть убеждён в его подлинности и в отсутствии искажений, вызванных чрезмерным сжатием данных.

Одним из распространённых подходов к решению задачи защиты изображений от изменений является встраивание полухрупких цифровых водяных знаков (ЦВЗ), которые сохраняются при незначительных изменениях изображения и уничтожаются в случае существенных модификаций. Однако в литературе можно найти лишь единичные примеры методов полухрупких ЦВЗ для изображений в формате JPEG 2000. В данной работе предлагается такой метод для режима сжатия JPEG 2000 с потерями, основанный на методе встраивания информации с переквантованием.

Сжатие с потерями в стандарте JPEG 2000

На первом этапе компрессии происходит сдвиг яркости каждой компоненты на -128. Затем осуществляется перевод из цветового пространства RGB в YCbCr. Полученное изображение подвергается дискретному вейвлет-преобразованию (ДВП) с банком фильтров Добеши (9, 7) для разбиения изображения на высокочастотные и низкочастотные области (поддиапазоны) [2].

После того, как вейвлет-преобразование масштаба вычислено, каждый коэффициент $a_b(u,v)$ поддиапазона b квантуется по формуле:

$$q_b(u,v) = \left\lfloor \left| \frac{a_b(u,v)}{\Delta_b} \right| \right\rfloor * sign(a_b(u,v)), \quad (1)$$

где $a_b(u,v)$ – коэффициенты квадрантов, Δ_b – шаг квантования.

Шаг квантования представляется двумя байтами: 11-битной мантиссой μ_b и 5-битным показателем ε_b, с и определяется по следующей формуле:

$$\Delta_b = 2^{R_b-\varepsilon_b}\left(1+\frac{\mu_b}{2^{11}}\right), \quad (2)$$

где R_b – номинальный динамический диапазон поддиапазона b.

Для сжатия с потерями стандартом допускается неявный расчёт пары (ε_b, μ_b) на основе заданных значений $(\varepsilon_0, \mu_0) \triangleq (\varepsilon, \mu)$, определённых для LL-поддиапазона, в соответствии с выражениями

$$\varepsilon_b = \varepsilon - N_L + n_b;\ \mu_b = \mu, \quad (3)$$

где N_L – общее число уровней декомпозиции, а n_b – номер уровня, соответствующий поддиапазону b [3].

Финальным шагом процесса сжатия является безошибочное кодирование квантованных коэффициентов с помощью метода арифметического кодирования на основе битовых плоскостей.

Декодер JPEG 2000 обращает описанные выше операции [3].

Встраивание информации на основе метода QIM

Для встраивания ЦВЗ было принято решение модифицировать операцию квантования (1), чтобы попутно при квантовании осуществлялось встраивание информации. Для этого был выбран метод QIM (Quantization Index Modulation) в форме алгоритма DM-QIM [4], адаптированного под формулу квантования (1). Алгоритм DM-QIM предполагает использование двух параметров – массивов подмешиваемых значений, согласованных друг с другом и используемых при встраивании битов «0» и «1»:

$$d_0(k), d_1(k) \epsilon \left[-\frac{\Delta}{2}; \frac{\Delta}{2} - 1\right], k \epsilon [0, K-1],$$

где K – количество квантуемых отсчётов.

Встраивание информации в алгоритме DM-QIM осуществляется по формуле:

$$y(k) = \Delta \cdot round\left(\frac{x(k) + d_{W(k)}(k)}{\Delta}\right) - d_{W(k)}(k), \quad (4)$$

где $x(k)$ – квантуемые отсчёты, а $W(k)$ – отсчёты водяного знака.

Для адаптации к стандарту сжатия JPEG 2000 формула (4) была изменена на следующую:

$$y(k) = sign\big(x(k)\big) \cdot \left(\Delta \cdot \left\lfloor \frac{x(k)+0.5\cdot\Delta\cdot sign\big(x(k)\big)+d_{W(k)}(k)}{\Delta} \right\rfloor - d_{W(k)}(k)\right), \quad (5)$$

При применении в процессе сжатия в качестве $x(k)$ используются значения $a_b(u,v)$, а в качестве шагов квантования Δ – значения Δ_b (см. (1)). Полученные квантованные значения $y(k)$ затем используются в качестве значений $q_b(u,v)$.

Зависимость функции встраивания информации от шага квантования Δ позволяет обеспечить требуемое условие полухрупкости ЦВЗ: информация должна сохраняться при сжатии с шагами квантования, меньшими Δ, и теряться при шагах, превышающих Δ.

Проверка работоспособности

Для проверки разработанного метода произведём встраивание ЦВЗ в изображение "Lenna". На рисунке 1 слева расположено исходное изображение, справа – со встроенным ЦВЗ. Визуально искажения, вызванные встраиванием не заметны.

Рисунок 1 – Исходное изображение (слева) и изображение со встроенным ЦВЗ (справа) (параметры квантования $\mu = 8.5$, $\varepsilon = 9$)

Далее убедимся, что ЦВЗ обладает свойством полухрупкости. Пусть W – встроенный водяной знак, а W^R – извлеченный, тогда точность извлечения будем вычислять по формуле (5):

$$\rho = 1 - \frac{1}{K}\sum_{k=0}^{K-1} XOR(W(k), W^R(k)) \quad (6)$$

На рисунке 2 отображены результаты эксперимента, в котором изображение во встроенным водяным знаком подвергалось сжатию JPEG 2000 с различ-

ными шагами квантования Δ_b, определяемыми значениями ε согласно формулам (2)-(3) (при фиксированном $\mu = 8.5$). После сжатия осуществлялась попытка извлечения ЦВЗ с последующим расчётом значения ρ. Как видно из графиков ЦВЗ сохраняется при меньшем шаге квантования (соответствующем большему значению ε, чем то, которое использовалось при сжатии). Таким образом, метод показал свою работоспособность в смысле обеспечения полухрупкости ЦВЗ.

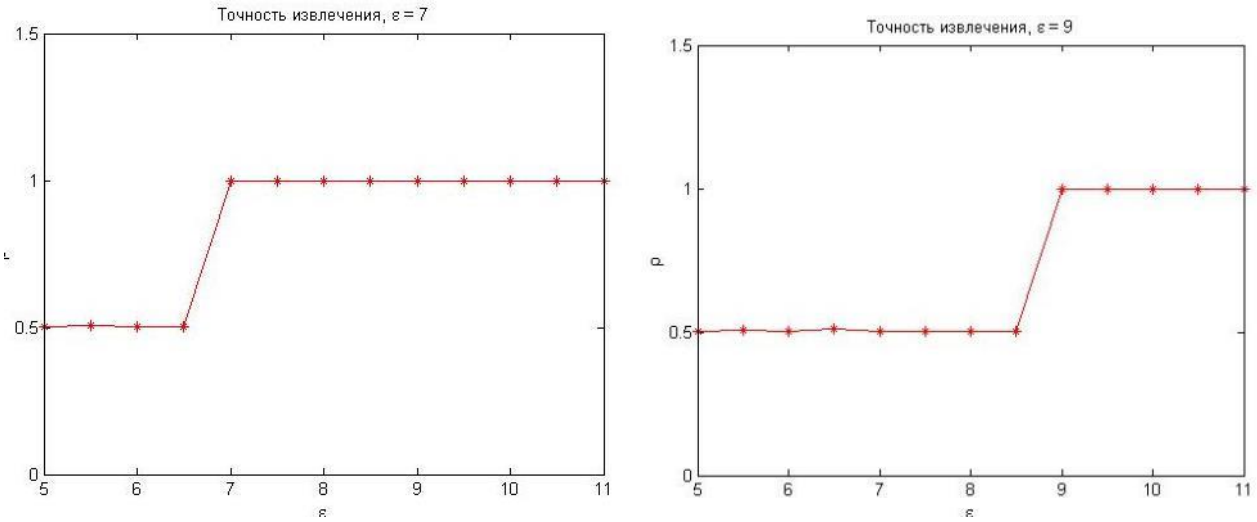

Рисунок 2 – Зависимость точности извлечения ЦВЗ от параметра ε (слева ЦВЗ встроен с параметрами $\mu = 8.5$, $\varepsilon = 7$, справа – с параметрами $\mu = 8.5$, $\varepsilon = 9$)

Далее исследуем объективный объем внесенных искажений с помощью показателя PSNR, а также качество изображения со встроенной информацией с точки зрения его восприятия человеком по критерию PSNR-HVS [5]. На рисунке 3 отображены результаты расчётов для изображения с рис. 1 и различных ε (μ фиксировано и равно 8.5), показывающие, что изображение не претерпевает существенной деградации ни по одному из показателей.

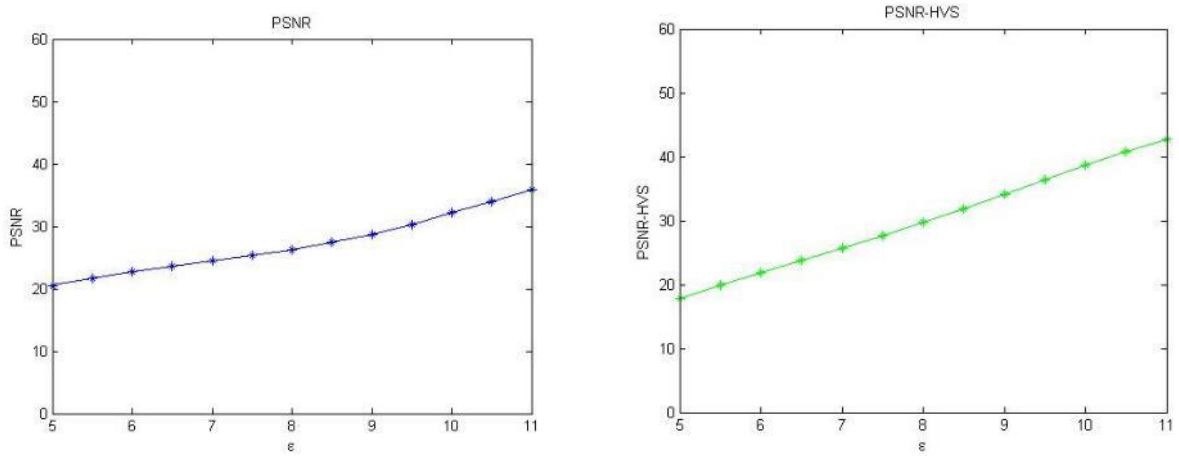

Рисунок 3 – Зависимость показателей качества изображения со встроенной информацией (PSNR слева и PSNR-HVS справа) от параметра ε, определяющего шаг квантования при встраивании ЦВЗ

Заключение

Предложенный метод встраивания полухрупких ЦВЗ показал свою работоспособность и может исследоваться далее на предмет возможности практического использования для защиты изображений в формате JPEG 2000.

Благодарности

Работа выполнена при поддержке Минобрнауки РФ в рамках гранта президента РФ МК-1907.2017.9.

Литература

1. JPEG 2000 [Электронный ресурс]. – JPEG. – Режим доступа: https://jpeg.org/jpeg2000/, свободный. – яз. англ.

2. Гонсалес, Р. Цифровая обработка изображений в среде MATLAB [Текст] / Р. Гонсалес, Р. Вудс, С. Эддинс. – М.: Техносфера, 2006. – 616с.

3. Rabbani, M. An overview of the JPEG 2000 still image compression standart [Text] / M. Rabbani, R. Joshi // Signal Processing: Image Communication. – 2004. - № 17. – 3-38 p.

4. Chen, B. Quantization index modulation: A class of provably good methods for digital watermarking and information embedding / B. Chen and G.W. Wornell // IEEE Transactions on Information Theory. – 2001. – V. 47(4). – P. 1423–1443. – DOI: 10.1109/18.923725.

5. Egiazarian, K. New full-reference quality metrics based on HVS [Text] / K. Egiazarian, J. Astola, N. Ponomarenko et al. // Proceedings of the Second International Workshop on Video Processing and Quality Metrics, Scottsdale, USA. – 2006. – 4 p.

Д.А. Бизин, С.А. Бурлов

МОДЕЛЬ КВАНТОВОГО АЛГОРИТМА ШИФРОВАНИЯ НА СОСТОЯНИЯХ ОРБИТАЛЬНОГО УГЛОВОГО МОМЕНТА ФОТОНОВ

(Самарский университет)

Орбитальный угловой момент (ОУМ) фотона – самая перспективная и исследуемая на сегодняшний момент физическая величина для передачи информации по квантовому каналу связи. В данной работе описана система шифрования на состояниях ОУМ фотонов.

В качестве измерительного прибора ОУМ рассматривается каскад интерферометров, рассмотренный в работе [1]. Каскад интерферометров формально будет не измерять состояния ОУМ фотонов, а сортировать их в зависимости от величин ОУМ по определенному модулю. В качестве алгоритма шифрования используется адаптированная схема Меркли, описанная в работе [2], использующая в качестве шифртекста смешанное состояние фотонов.

Каждый фотон имеет азимутальную фазовую зависимость вида $e^{il\varphi}$, на которую будет ориентироваться каскад интерферометров. Такие фотоны несут