Мультиплексирование скрытых каналов при реализации стеганографического встраивания в цифровые изображения с использованием некриптографических хеш-функций

М. А. Дрюченко, email: m_dryuchenko@mail.ru [1]

[1] Воронежский государственный университет

Аннотация. *В данной работе рассматривается алгоритм стеганографического скрытия информации в пространственном представлении цифровых изображений, основанный на использовании некриптографических хеш-функций для извлечения данных. Алгоритм не является робастным, но характеризуется малым соотношением числа модифицируемых бит контейнера к числу встраиваемых бит сообщения, что позволяет обеспечить минимальные визуальные и статистические искажения стегоконтейнеров. Описывается модификация алгоритма встраивания, позволяющая создавать несколько скрытых каналов, использующих общее подмножество элементов контейнера при встраивании в них сообщений, предназначенных для различных пользователей.*

Ключевые слова: *стеганографическое скрытие информации, некриптографические хеш-коды.*

Введение

Современные методы цифровой стеганографии позволяют эффективно решать задачи по защите конфиденциальности данных, организации защищенных скрытых каналов передачи информации, защите авторских прав, контроле целостности и аутентичности данных. В числе обязательных требований, предъявляемых к стегоалгоритмам, можно отметить минимизацию вносимых в процессе стегоскрытия искажающих изменений контейнеров. Вторым возможным требованием к стегоалгоритмам может выступать высокая скрытная пропускная способность (ПС) $ПС = |M|/|I|$, оцениваемая как отношение размера скрываемого сообщения M к размеру контейнера I. На практике совместить данные требования в рамках одного стегоалгоритма достаточно сложно – повышение ПС чаще всего реализуется за счет модификации большего числа элементов контейнера, что в свою очередь приводит к нежелательному увеличению его искажений.

Современные алгоритмы пространственной стеганографии [1-4] реализуют идею адаптивного внедрения сообщений, решая задачу минимизации искажений путем целенаправленного выбора для внедрения данных наиболее стохастичных областей контейнера, искажения в которых достаточно сложно обнаружить не только визуально, но и с привлечением современных методов стегоанализа. К ограничениям подобных алгоритмов можно отнести невысокую ПС, а также (зачастую) необходимость наличия оригинальных незаполненных контейнеров для извлечения сообщений. Алгоритмы стохастической модуляции [5-7], минимизируют не абсолютные искажения контейнеров, а их статистические отличия от естественных незаполненных контейнеров путем внесения в них дополнительных шумов с заданными вероятностными распределениями, имитирующих шумы естественных контейнеров. При сопоставимой ПС уровень искажений маркированных алгоритмами стохастической модуляции контейнеров может быть значительно выше, чем для алгоритмов адаптивного пространственного скрытия. Современные алгоритмы, реализующие принцип Steganography Without Embedding «стеганография без встраивания» [8,9], не реализуют классического встраивания данных с модификацией элементов контейнера, не маскируют присутствие полезного сигнала под шумами, а с помощью специально обученных моделей машинного обучения (генеративно состязательных сетей) формируют синтетические заполненные контейнеры, из которых сообщение может быть извлечено обученными сетями-экстракторами. Подобные алгоритмы имеют достаточно высокую ПС и показывают хорошие результаты в части противодействия стегоанализу, однако они имеют существенные ограничения, связанные с необходимостью настройки и передачи достаточно больших моделей, а также невозможностью использования имеющихся контейнеров.

В данной работе рассматривается алгоритм стеганографического скрытия в пространственном представлении цветных изображений, позволяющий встраивать сообщения, длина которых существенно превышает число модифицируемых элементов носителя, что позволяет повысить ПС при минимальных итоговых искажениях маркированных контейнеров. Алгоритм предусматривает разбиение контейнера-изображения на непересекающиеся блоки с поиском для каждого из них такого минимально искаженного представления, которое обеспечивает корректное извлечение фрагмента сообщения – слова заданной разрядности. В процедуре извлечения ранее скрытых данных используется т.н. функция «свертки» $н$, применяемая к блокам

пикселей для их преобразования в значения фиксированной длины (слова сообщения). В качестве функции H, обеспечивающей требуемое преобразование входных данных, рассматривались некриптографические хеш-функции, характеризующиеся высоким быстродействием и хорошими стохастическими свойствами формируемых выходных значений. Для практической реализации стегоалгоритма была выбрана некриптографическая хеш-функция Murmur3 [10].

При разработке стегоалгоритма отдельное внимание было уделено вопросам мультиплексирования скрытых каналов. Был предложен вариант создания пары скрытых каналов, формируемых одновременно с использованием одного и того же подмножества элементов контейнера, позволяющих в несколько раз увеличить фактическую ПС алгоритма без необходимости внесения в блоки контейнера дополнительных существенных искажений.

1. Алгоритм встраивания данных

Рассмотрим алгоритм встраивания в режиме мультиплексирования каналов на примере создания в контейнере двух скрытых каналов C_M и C_S, используемых для передачи независимых сообщений M и S. $M = m_1^{(n)} || m_2^{(n)} || \cdots m_{N_M}^{(n)}$, N_M – число n-битных слов, составляющих скрываемое сообщение M, $S = s_1^{(v)} || s_2^{(v)} || \cdots s_{N_S}^{(v)}$, N_S – число v-битных слов, составляющих сообщение S. Укрупненная блок-схема алгоритма встраивания приведена на рис. 1. Она включает следующие шаги.

Шаг 1. Загрузка сообщений M и S. Добавление целочисленных значений длин каждого сообщения в его начало. Задание размеров обрабатываемых блоков контейнера, разрядности скрываемых слов n и v, параметров для инициализации генераторов псевдослучайных числовых последовательностей (ГПСЧП), рандомизирующих встраиваемые слова и определяющих порядок обхода блоков при встраивании сообщений.

Шаг 2. Выбор на I очередного блока b_i и оценка его «гладкости». Модификация гладких блоков отрицательно отражается на визуальной и статистической незаметности факта стегоскрытия, поэтому в первую очередь в алгоритме модифицируются шумные блоки, допускающие потенциально большие искажения, которые с меньшей вероятностью могут быть обнаружены при стегоанализе. В качестве параметра гладкости блока использовалось среднее значение дисперсий, вычисленных для модулей градиента блока в каждом его канале

$c_i = \frac{1}{3}\sum_{ch=R,G,B} D\left(grad\left(b_{i,ch}\right)\right)$. Если гладкость i -го блока $c_i < 0.15$, то он пропускаются и осуществляется переход в начало шага 2. Если блок подходит для встраивания выбирается очередное n -битное слово $m_i^{(n)} \in M$ и выполняется его рандомизация $\tilde{m}_i^{(n)} = m_i^{(n)} \oplus r_i^{(n)}$, $r_i^{(n)}$ – n -битное значение на выходе ГПСЧП-1.

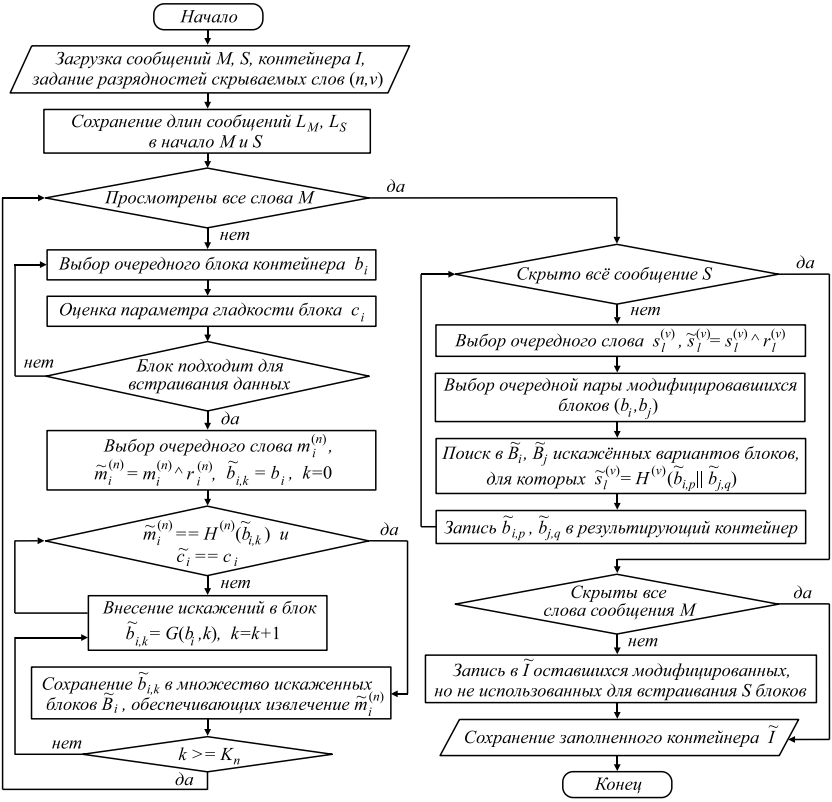

Рис. 1. Обобщенная схема алгоритма встраивания данных при создании двух скрытых каналов

Шаг 3. Вычисление множества различных вариантов искажений блока b_i $\tilde{B}_i = \left\{\tilde{b}_{i,1}, \cdots \tilde{b}_{i,N_i}\right\}$, таких, что

$$H^{(n)}\left(\tilde{b}_{i,k}\right) = \tilde{m}_i^{(n)}, \ \tilde{c}_i \neq 0, \ \forall\, k = \overline{1, N_i}. \qquad (1)$$

Элементы $\tilde{B}_i$ являются коллизиями для функции $H^{(n)}$ (N_i – число коллизий) и каждый из $\tilde{b}_{i,k}$ обеспечивает корректное извлечение слова $\tilde{m}_i^{(n)}$. Для модификации элементов b_i применяется функция G вида

$$\tilde{b}_{i,k} = G(b_i, k) = \left(b_i(1) + \psi_{1,k},\ b_i(2) + \psi_{2,k}, \cdots, b_i(L_b) + \psi_{L_b,k}\right), \qquad (2)$$

которая, в зависимости от текущего значения переменной счетчика k, добавляет к значениям цветов пикселей блока элементы вектора $\Psi_k = \left(\psi_{1,k}, \cdots \psi_{L_b,k}\right)^T$, где $\psi_{j,k}$, $j = \overline{1, L_b}$ могут принимать значения $\{0, \pm 1, \pm 2, \cdots \pm \lambda\}$, λ – максимальное значение, добавляемое к значению цвета пикселя (обычно $\lambda \le 3$), $L_b = 3 \cdot w \cdot h$ – число доступных для модификации элементов блока для полноцветных контейнеров. Векторы Ψ_k, $k = \overline{1, K}$ формируются таким образом, чтобы при малых k количество и уровень вносимых изменений в b_i были минимальными. С увеличением k число одновременно модифицируемых коэффициентов в b_i, а также абсолютные значения приращений $\psi_{j,k}$ постепенно увеличиваются.

Если просмотрены не все слова из M выполняется переход к шагу 2.

Шаг 4. Выбор очередного v-битного слова из второго скрываемого сообщения $s_l^{(v)} \in S$, $\tilde{s}_l^{(v)} = s_l^{(v)} \oplus r_l^{(v)}$, $r_l^{(v)}$ – v-битное значение на выходе ГПСЧП-2.

Шаг 5. Согласно ГПСЧП-3 выбор очередной пары модифицировавшихся блоков b_i, b_j. Поиск в сформированных на шаге 3 множествах вариантов искажений $\tilde{B}_i$ и $\tilde{B}_j$ элементов, для которых справедливо

$$\tilde{s}_l^{(v)} = H^{(v)}\left(\tilde{b}_{i,p} \,||\, \tilde{b}_{j,q}\right),\ \left\|b_i - \tilde{b}_{i,p}\right\| \to \min,\ \left\|b_j - \tilde{b}_{j,q}\right\| \to \min, \qquad (3)$$

где $||$ – операция конкатенации блоков (на уровне байтовых массивов), $H^{(v)}$ – некриптографическая хеш функция с финализированным выходом длиной v-бит. Запись содержимого модифицированных блоков $\tilde{b}_{i,p}$, $\tilde{b}_{j,q}$ на соответствующие позиции в результирующем контейнере $\tilde{I}$. Для обеспечения возможности встраивания и извлечения v-битных слов $\tilde{s}_l^{(v)}$, необходимо, чтобы число различных пар искаженных блоков b_i, b_j в (3), оцениваемое как произведение мощностей множеств $\tilde{B}_i$ и $\tilde{B}_j$,

было не меньше, чем 2^{v} (на практике, с учетом возможных коллизий в несколько раз больше).

Переход к шагу 4 если $l < N_S$, т.е. встроены не все слова из S.

Шаг 6. Если остались модифицировавшиеся на шаге 3, но не использованные для встраивания s блоки, из соответствующих им множеств $\tilde{B}_i$ осуществляется выбор и запись в результирующий контейнер искаженных представлений блоков $\tilde{b}_{i,p}$, минимально отличающихся от исходных $\left\| b_i - \tilde{b}_{i,p} \right\| \to \min$.

Шаг 7. Сохранение заполненного контейнера $\tilde{I}$.

В результате формируется заполненный контейнер $\tilde{I}$, с парой скрытых каналов передачи информации C_M и C_S. Особенностью предложенной схемы является одновременное формирование скрытых каналов на основе одного и того же подмножества модифицируемых элементов носителя. Соотношение между длинами сообщений M и S может быть произвольным: $|M| > |S|$, $|M| < |S|$, $|M| = |S|$, все зависит от выбранной разрядности скрываемых слов каждого сообщения. Например, если $n = 4$, а $v = 16$ и для скрытия используются все подходящие блоки контейнера, то $|S| = 2|M|$. Соотношение между числом модифицируемых блоков контейнера подчиняется неравенству $N_S \le N_M / 2$.

Схематичная графическая интерпретация операций встраивания/извлечения данных из первого и второго скрытых каналов приведена на рис. 2.

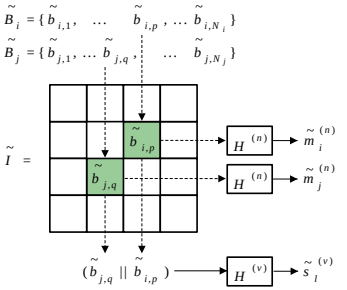

Рис. 2. Пример выбора искаженных блоков, обеспечивающих извлечение данных из первого и второго скрытых каналов

Пример исходных и модифицированных в режиме мультиплексирования скрытых каналов блоков контейнера при

встраивании пар 8-битных слов в C_M и 8-битных слов в C_S приведен на рис. 3. В качестве $H^{(8)}$ использовалась некриптографическая хеш-функция Murmur3 с финализацией выхода по разрядности встраиваемых слов ($seed = 135$), $\lambda \le 2$, $N_{corr} \le 3$.

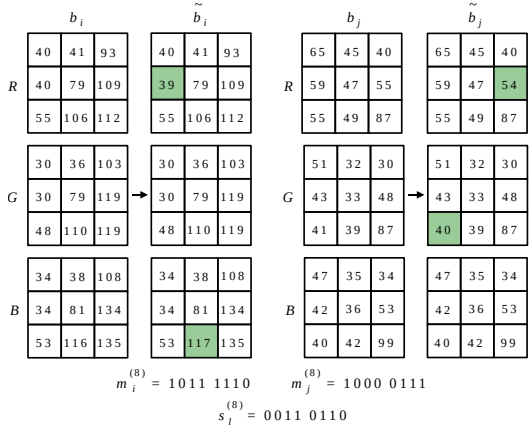

Рис. 3. Пример выбора искаженных блоков, обеспечивающих извлечение данных из первого и второго скрытых каналов

2. Алгоритм извлечения данных

Схема алгоритма извлечения данных приведена на рис. 4. Данный алгоритм не требует наличия исходного незаполненного контейнера, отличается вычислительной простотой и включает следующие шаги.

Шаг 1. Загрузка заполненного контейнера $\tilde{I}$.

Шаг 2. Согласно ГПСЧП-3 выбор на $\tilde{I}$ очередной пары блоков $\tilde{b}_i, \tilde{b}_j$, оценка их гладкости (гладкие блоки пропускаются и выполняется переход в начало шага 2).

Шаг 3. Извлечение и декодирование слова $\tilde{s}_l^{(v)} = H^{(v)}\left(\tilde{b}_i \,||\, \tilde{b}_j\right)$, $s_l^{(v)} = \tilde{s}_l^{(v)} \oplus r_l^{(v)}$. Если длина сообщения S не сформирована запись $s_l^{(v)}$ в соответствующую целочисленную переменную L_S. Иначе запись $s_l^{(v)}$ в результирующее сообщение S. Извлечение и декодирование слов $\tilde{m}_i^{(n)} = H^{(n)}\left(\tilde{b}_i\right)$, $m_i^{(n)} = \tilde{m}_i^{(n)} \oplus r_i^{(n)}$, $\tilde{m}_j^{(n)} = H^{(n)}\left(\tilde{b}_j\right)$, $m_j^{(n)} = \tilde{m}_j^{(n)} \oplus r_j^{(n)}$. Если длина сообщения M не сформирована запись слов $m_i^{(n)}, m_j^{(n)}$ в

соответствующую целочисленную переменную L_M. Иначе запись $m_i^{(n)}$, $m_j^{(n)}$ в результирующее сообщение M.

Если число извлеченных байт в S меньше L_S или S число извлеченных байт в M меньше L_M переход к шагу 2.

Шаг 4. Сохранение сообщений M и S.

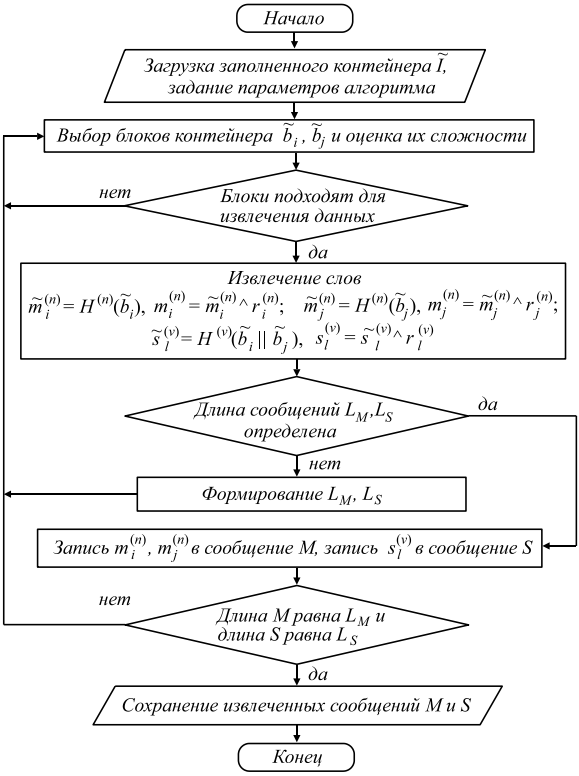

Рис. 4. Пример выбора искаженных блоков, обеспечивающих извлечение данных из первого и второго скрытых каналов

В общем случае каналы C_M и C_S могут использоваться для скрытной передачи данных любого характера, предназначенных различным абонентам. Особенность формирования скрытых каналов на основе одного и того же подмножества элементов контейнера допускает использование C_M как второстепенного несекретного канала,

маскирующего наличие C_S, содержащего конфиденциальную информацию.

Заключение

Описанные в статье принципы скрытия и извлечения данных являются универсальными и могут применяться как в пространственном, так и в частотном [11] представлении контейнеров различных форматов. Алгоритм скрытия характеризуется достаточно высокой ПС и на практике способен обеспечить соотношение числа фактически модифицируемых бит контейнера к числу встраиваемых бит сообщения порядка 0,06, в то время как для большинства современных алгоритмов стегоскрытия данный показатель находится на уровне от 0,5 и выше. ПС алгоритма может варьироваться в зависимости от размеров искажаемых блоков, разрядности встраиваемых слов, характера содержимого маркируемых контейнеров, определяющего процент пропускаемых при скрытии блоков. Главной особенностью предложенной схемы мультиплексирования скрытых каналов является использование одного и того же подмножества элементов, подвергающихся одинаковым искажениям при встраивании различных сообщений, что позволяет увеличить ПС и снизить общий уровень вносимых в контейнер искажений.

Список литературы

1. Holub, V. Designing steganographic distortion using directional filters / V. Holub, J. Fridrich // Proc. 4th IEEE Intern. Workshop on Inform. Forensics and Security (WIFS), Tenerife, Spain, 2012. – P. 234-239. DOI: 10.1109/WIFS.2012.6412655.
2. Holub, V. Digital image steganography using universal distortion / / V. Holub, J. Fridrich // Proc. 1st ACM Workshop on Inform. Hiding and Multimedia Security (IHMMSec), Montpellier, France, 2013. – P. 59-68. DOI: 10.1145/2482513.2482514.
3. Pevn´y, T. Using high-dimensional image models to perform highly undetectable steganography / T. Pevn´y, T. Filler, P. Bas // LNCS, 2010. – P. 161-177. DOI: 10.1007/978-3-642-16435-4_13.
4. Keyless dynamic optimal multi-bit image ste-ganography using energetic pixels / G. Paul [et al.] // Multimedia Tools and Applications, 76(5), 2017. – P. 7445-7471. DOI: 10.1007/s11042-016-3319-0.
5. Fridrich, J. Digital image steganography using stochastic modulation / J. Fridrich, M. Goljan // Proceedings of SPIE - The International Society for Optical Engineering, 2003. DOI: 10.1117/12.479739.
6. Елтышева, Е.Ю. Построение стегосистемы для растровых изображений на основе стохастической модуляции с учетом статистики

младших бит / Е.Ю. Елтышева // Вестник СибГУТИ. – 2011. – №2. – С. 63-75.

7. Сирота, А.А. Метод создания цифровых водяных знаков на основе гетероассоциативных сжимающих преобразований изображений и его реализация с использованием искусственных нейронных сетей / А.А. Сирота, М.А. Дрюченко, Е.Ю. Митрофанова // Компьютерная оптика. – 2018. – №3. – С. 483–494.

8. A Novel Image Steganography Method via Deep Convolutional Generative Adversarial Networks / H. Donghui [et al.] // IEEE Access, 2018. – Vol.6. – P. 38303-38314. DOI: 10.1109/ACCESS.2018.2852771.

9. Generative Steganography Network / W. Ping [et al.] // Proceedings of the 30th ACM International Conference on Multimedia, 2022. – P. 1621-1629. DOI: 10.1145/3503161.3548217.

10. Appleby, A. Murmurhash3 – non-cryptographic hash [Электронный ресурс]. – Режим доступа : https://github.com/aappleby/smhasher/.

11. Дрюченко, М.А. Алгоритм стеганографического скрытия данных в jpeg изображения, основанный на использовании функций свертки / М.А. Дрюченко // Вестник Воронежского государственного университета. Серия: Системный анализ и информационные технологии. – 2018. – № 3. – С. 93–102.