Гипотеза 1 [1]. Существуют υ-алгоритмы шифрования Фейстеля, где $\upsilon \in \left\{\upsilon^{(1)}, \upsilon^{(2)}\right\}$, у которых при любом числе раундов $l \geqslant n^2$ отсутствуют невозможные усечённые разности.

Нами получено нетривиальное доказательство этой гипотезы. Кроме того, получено существенное её усиление, а именно доказана следующая теорема.

Теорема 1. Пусть υ — произвольная функция из множества Υ_n, $\upsilon(n) = e$, и υ-алгоритм Фейстеля независим. Пусть также для всех $i \in \{\overline{1,n}\}_\upsilon$ множество $H_i^\upsilon \subseteq P(V_m)$ таково, что $\tilde{\pi}_{\delta_1\delta_2}(H_i^\upsilon) = 1$ для всех $(\delta_1, \delta_2) \in V_m^* \times V_m$. Тогда для произвольных разностей $\theta, \theta' \in (V_m^n)^*$ и произвольного вектора $\alpha \in V_m^n$ для любого $l \geqslant n^2$ существует преобразование $h \in \left\{g_{k(l)}^{(\upsilon)} | k(l) \in \mathrm{K}_\upsilon^l\right\}$, удовлетворяющее равенству $\alpha^h \oplus (\alpha \oplus \theta)^h = \theta'$.

Также показано, что для произвольного независимого υ-алгоритма Фейстеля, при условии 2-транзитивности множеств $H_i^\upsilon \subseteq P(V_m)$ для всех $i \in \{\overline{1,n}\}_\upsilon$, оценка его показателя 2-транзитивности совпадает с оценкой числа раундов, на котором отсутствуют невозможные разности.

ЛИТЕРАТУРА

1. *Sung J., Lee S., Lim J. et al.* Security for the Skipjack-like Structure against Differential Cryptanalysis and Linear Cryptanalysis // ASIACRYPT'2000, LNCS. 2000. V. 1976. P. 274–288.
2. *Feistel H., Notz W.* Some cryptographic techniques for machine-to-machine data communications // Proc. IEEE. 1975. V. 63. No. 11. P. 1545–1554.
3. *Schnorr C. P.* On the construction of random number generators and random function generators // Advances in Cryptology. Proc. Eurocrypt-88, LNCS. 1988. V. 330. P. 225–232.
4. *Zheng Y., Matsumoto T., Imai I.* On the construction of block ciphers provably secure and not relying on any unproved hypotheses // Crypto-89, LNCS. 1989.
5. *Moriai S., Vaudenay S.* On the pseudorandomness of top-level schemes of block ciphers // ASIACRYPT'2000, LNCS. 2000. V. 1976. P. 289–302.
6. *Schneier B., Kelsey J.* Unbalanced feistel networks and block cipher design // FSE, 3rd International Workshop. Springer Verlag, 1996. P. 121–144.

УДК 621.391.037.372

АНАЛИЗ СТЕГОСИСТЕМ С НАРУШЕНИЕМ КВАНТОВАНИЯ

Е. В. Разинков, Р. Х. Латыпов

Основная задача стеганографии — обеспечение скрытой передачи информации, достигаемой встраиванием секретного сообщения в не привлекающий внимания объект, который и передается по каналу связи [1, 2]. Основные средства, которыми располагает нарушитель — статистические и визуальные атаки. Если визуальная атака направлена на обнаружение секретного сообщения путем исследования стегосообщения человеком, его органами чувств, то статистическая атака основывается на исследовании статистических характеристик цифрового объекта, которые нарушаются в результате сокрытия информации [2].

Один из способов повысить устойчивость стеганографической системы — адаптивный выбор элементов стегоконтейнера для встраивания информации [2 – 5]. К примеру, информация может встраиваться в наиболее зашумленные участки изображения, что усложняет ее обнаружение нарушителем. Следует заметить, однако, что адаптивное

правило выбора элементов контейнера чаще всего не зависит или слабо зависит от секретного ключа [3]. Это свойство позволяет и нарушителю провести успешную атаку на стегосистему. Проблема может быть решена, если при встраивании используется информация, доступ к которой нарушитель получить не может. Такой подход к сокрытию информации, позволяя использовать преимущества адаптивного стеганографического преобразования, не понижает устойчивости системы, так как нарушитель не имеет возможности применить правило выбора элементов стегоконтейнера. Извлечение сообщения получателем возможно благодаря так называемым «wet paper codes», предложенным в [6].

Идея стеганографии с нарушением квантования состоит в использовании информации, отбрасываемой в результате обработки стегоконтейнера с потерями. Речь идет об уменьшении размеров изображения, о сокращении цветовой гаммы, о JPEG-преобразовании [3]. В данной статье анализируется использование стеганографии с нарушением квантования для сокрытия информации в JPEG-изображениях, поэтому именно этот метод рассмотрен ниже.

Как известно, в процессе проведения JPEG-преобразования применяется дискретное косинусное преобразование (DCT — Discrete Cosine Transform), коэффициенты которого подвергаются делению на элементы матрицы квантования и округлению до ближайшего целого. В [3] предлагается для встраивания информации использовать коэффициенты, лежащие в интервале $(n+0{,}5-\varepsilon; n+0{,}5+\varepsilon)$, где ε — некоторое небольшое положительное число (например, $\varepsilon = 0{,}1$), а n — целое. Для этих коэффициентов, называемых *изменяемыми*, ошибка округления максимальна и не меняется значительно при изменении коэффициента (если значение округленного коэффициента меняется с n на $n+1$ или, наоборот, с $n+1$ на n).

Авторы вышеизложенного метода докладывают о высокой устойчивости стеганографии с нарушением квантования к атакам, направленным на обнаружение наличия скрытого сообщения. Основной недостаток метода заключается в следующем: отправитель вынужден либо использовать несжатые изображения в качестве стеганографических контейнеров (что не всегда удобно), либо пересылать получателю дважды сжатое с помощью JPEG-компрессии изображение (что повышает подозрительность стегосообщения) [3].

Исследование, предлагаемое в данной статье, представляет собой анализ стегосистем с нарушением квантования. Задача состоит в нахождении способа определения изменяемых коэффициентов на основе уже квантованных коэффициентов, то есть на основе лишь JPEG-представления изображения.

Мы выдвигаем следующее естественное предположение: искажения, вносимые модификацией коэффициента, не относящегося к изменяемым, в сторону увеличения и в сторону уменьшения, должны быть ближе друг к другу по величине, нежели искажения, вносимые аналогичными модификациями изменяемого коэффициента.

Пусть $d(c_{u,v} = x)$ — мера «неестественности» изображения при значении x коэффициента $c_{u,v}$ (в [7] поясняется обоснованность использования этого понятия). Тогда изложенное выше предположение можно записать следующим образом.

Пусть $c_{u,v}$ — изменяемый коэффициент, $c_{u,v} \in (n+0{,}5-\varepsilon; n+0{,}5+\varepsilon), \mathrm{round}(c_{u,v}) = n$. Тогда, в соответствии со сделанным предположением:

$$d(c_{u,v} = n) \approx d(c_{u,v} = n+1), d(c_{u,v} = n-1) \gg d(c_{u,v} = n+1).$$

Пусть $c_{\bar{u},\bar{v}} \approx n, \mathrm{round}(c_{\bar{u},\bar{v}}) = n$. Тогда $d(c_{\bar{u},\bar{v}} = n-1) \approx d(c_{\bar{u},\bar{v}} = n+1)$.

В качестве меры «неестественности» изображения мы предлагаем следующую функцию:

$$d = \sum_{i=1}^{i=7}\sum_{j=1}^{j=8} |b_{i,j} - b_{i+1,j}|^{1/2} + \sum_{i=1}^{i=8}\sum_{j=1}^{j=7} |b_{i,j} - b_{i,j+1}|^{1/2}.$$

Здесь $b_{i,j}$ — значения яркостей пикселей блока, содержащего исследуемый коэффициент c; они зависят от c следующим образом:

$$b_{i,j} = \text{round}\left(\frac{1}{4}\sum_{u=0}^{u=7}\sum_{v=0}^{v=7} p_u p_v c_{u,v} q_{u,v} cos\frac{(2j+1)u\pi}{16}\cos\frac{(2i+1)v\pi}{16}\right), \qquad (1)$$

где $p_0 = 1/\sqrt{2}$; $p_u = 1$ при $u > 0$. Вычислять d для всего изображения смысла не имеет, так как изменение JPEG-коэффициента влияет только на содержащий его блок размером 8×8 пикселей.

Результаты проведенных экспериментов показывают, что предположение подтвердилось для ненулевых JPEG-коэффициентов. Предлагается выбирать те ненулевые JPEG-коэффициенты $c_{u,v}$, для которых выполняется следующее неравенство:

$$|d(c_{u,v} = n - 1) - d(c_{u,v} = n + 1)| > M,$$

где M — константа, от величины которой зависит количество коэффициентов в выборке и процентное содержание в выборке изменяемых коэффициентов. Эксперименты показывают, что предлагаемый метод позволяет получать выборки, концентрация изменяемых коэффициентов в которых достигает 70 %.

Полученные в данной работе результаты могут быть применены для построения стегосистемы, использующей преимущества стеганографии с нарушением квантования, но не нуждающейся в несжатых изображениях — в качестве стеганографического контейнера можно использовать изображения в формате JPEG без изменения параметров JPEG-преобразования.

ЛИТЕРАТУРА

1. *Simmons G. J.* The PrisonersṔroblem and the Subliminal Channel // CRYPTO83 — Advances in Cryptology. New York: Springer, 1984. P. 51–67.
2. *Wayner P.* Disappearing Cryptography, Second Edition — Information Hiding: Steganography and Watermarking. San Francisco: Morgan Kaufmann, 2002. 413 p.
3. *Fridrich J., Goljan M., Soukal D.* Perturbed Quantization Steganography // ACM Multimedia & Security J. 2005. V. (11)2. P. 98–107.
4. *Fridrich J., Goljan M., Soukal D.* Perturbed Quantization Steganography with Wet Paper Codes // ACM Multimedia and Security Workshop. New York: ACM Press, 2004. P. 4–15.
5. *Fridrich J., Pevny T., Kodovsky J.* Statistically Undetectable JPEG Steganography: Dead Ends, Challenges, and Opportunities // ACM Multimedia and Security Workshop. New York: ACM Press, 2007. P. 3–14.
6. *Fridrich J., Goljan M., Lisonek P., Soukal D.* Writing on Wet Paper // IEEE Trans. on Sig. Proc., Special Issue on Media Security. 2005. V. 53. P. 3923–3935.
7. *Sullivan K., Madhow U., Chandrasekaran S., Manjunath B.S.* Steganalysis for Markov cover data with applications to images // IEEE Transactions on Information Forensics and Security. 2006. V. 1. No. 2. P. 275–287.