учитывать, что при увеличении выборки обучения, значительно возрастает время обучения. Так же можно столкнуться с проблемой переобучения нейронной сети, которое возникает в случае слишком долгого обучения, недостаточного числа обучающих примеров или переусложненной структуры нейронной сети. При данном явлении сеть теряет способность к обобщению и перестает быть гибкой.

Впоследствии имеет смысл провести подобное исследование для вероятностных распределений, которые лучше описывают поведение реальных сигналов, например, распределения Вейбулла, распределения Парето и др.

В дальнейшем на созданную и обученную нейронную сеть можно подавать не только зашумленные последовательности уже известных распределений, а так же неизвестные последовательности, например значения трафика, и относить их с некой вероятностью к распределениям, которые имеются в «памяти» нейронной сети.

Список используемых источников

1. Медведев В. С., Потемкин В. Г. Нейронные сети. Matlab 6. М.: Диалог-МИФИ, 2002. 496 с. ISBN 5-86404-163-7.

2. Christopher M. Bishop. Neural Networks for Pattern Recognition, Clarendon press Oxford, 1995. 482 p.

3. Комашинский В. И., Смирнов Д. А. Нейронные сети и их применение в системах управления и связи. М.: Горячая линия-Телеком, 2003. 94 с. ISBN 5-93517-094-9.

4. Осовский С. Нейронные сети для обработки информации / пер. с польского И. Д. Рудинского. М.: Финансы и статистика, 2002. 344 с.: ил. ISBN 5-279-02567-4.

5. Учебник «СтатСофт» [Электронный ресурс] / URL: http://www.statsoft.ru/home/ textbook/ modules/stneunet.html

6. Круглов В. В., Борисов В. В. Искусственные нейронные сети: теория и практика. М.: Горячая линия-Телеком, 2002. 382 с. ISBN 5-93517-031-0.

СРАВНЕНИЕ ЭФФЕКТИВНОСТИ МЕТОДОВ ПОСТРОЕНИЯ СТЕГОСИСТЕМ С ИНФОРМИРОВАННЫМ КОДЕРОМ

К.С. Горышин, К.А. Небаева

В данной статье рассматриваются два метода построения стегосистем с информированным кодером: использующие улучшенные сигналы с расширенным спектром и квантованную проективную модуляцию/демодуляцию, приводится их сравнительный анализ скоростей вложения, вероятностей ошибочного извлечения бита сообщения, и вероятностей ложного обнаружения и пропуска СГС.

Ключевые слова: улучшенные сигналы с расширенным спектром, квантованная проективная модуляция, стеганография

COMPARATIVE EFFICIENCY ANALYSIS OF INFORMED ENCODER STEGOSYSTEMS BUILDING METHODS

Goryshin K., Nebaeva K.

This article considers two informed encoder stegosystems building methods. The first one uses improved spread spectrum signals, the second one uses quantized projective modulation/demodulation. The article represents comparative analysis of their embedding speeds, wrong information bit extraction probabilities, false alarm and stegosystem miss probabilities.

Keywords: improved spread spectrum signals, quantized projective modulation, steganography

В открытых публикациях [1, 2] описаны исследования стегосистем (СГС), предназначенных для использования в каналах с шумом, однако недостаток таких СГС заключается в том, что для извлечения информации необходимо использовать информированный декодер, т. е. получателю необходимо знать покрывающее сообщение (ПС) (файл, в который производилось вложение). Для того чтобы преодолеть данный недостаток в работе [3] предлагается использовать так называемый «слепой декодер», т. е. декодер, которому не требуется знание ПС. В таком случае необходимо производить вложение с использованием информированного кодера. Существуют два основных метода построения СГС с информированным кодером: так называемые *улучшенные сигналы с расширенным спектром* (*improved spread spectrum signals* (ISSS)) и *квантованная проективная модуляция* (*quantized projective modulation/demodulation* (QPD)).

Основная идея ISS [4] – уменьшить влияние ПС как помехи на результат «слепого» декодирования.

Погружение информации в методе ISS выполняется следующим образом:

$$C_w(n) = C(n) + (\beta(-1)^b - \lambda x)\pi'(n),\ n = 1,2,..,N_0, \qquad (1)$$

где $C(n)$ – ПС, $C_w(n)$ – стегосигнал (СГ), $b \in \{0,1\}$ – значение вкладываемого бита; β, λ – некоторые постоянные коэффициенты; $x = \frac{1}{N\alpha^2}\sum_{n=1}^{N_0} C(n)\pi'(n)$; $\pi'(n) = \alpha\pi(n)$, $\pi(n)$ – псевдослучайная последовательность (ПСП), $\alpha \in R$ – коэффициент глубины вложения, N_0 – длина блока ПС (количество отсчетов), в который вкладывается один бит сообщения. Для вложения последующих бит информации используются другие ПСП, которые не имеют простой вычислительной связи друг с другом.

Из выражения (1) видно, что погружение не является чисто аддитивным, а зависит от ПС на интервале N_0 отсчетов.

Извлечение информации производится слепым декодером по правилу:

$$\tilde{b} = \mathrm{rect}\left\{\sum_{n=1}^{N_0} C'_w(n)\pi'(n)\right\},$$

где $\mathrm{rect}\{x\} = \begin{cases} 0 \text{ при } x \geq 0 \\ 1 \text{ при } x < 0 \end{cases}$, $\tilde{b}$ – извлекаемый бит, $C'_w(n), n = 1,2,..,N_0$ – отсчеты СГ после возможной атаки аддитивным шумом, т.е.:

$$C'_w = C(n) + \varepsilon(n),$$

где $E\{\varepsilon(n)\} = 0, Var\{\varepsilon(n)\} = \sigma_\varepsilon^2$.

Вероятность ошибки при извлечении вложенной информации:

$$P = Q\left(\sqrt{\frac{N_0 - \eta_w}{\eta - 1}}\right),$$

где $\eta = \frac{\eta_w}{\eta_a}$, η_w – отношение сигнал/шум после вложения, η_a – отношение сигнал/шум после вложения и атаки. $Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty e^{\frac{-t^2}{2}} dt$.

Цель использования QPD – обеспечить защиту от преднамеренного удаления вложения методом рандомизированного квантования.

Погружение [3]:

$$C_w(n) = C(n) + \frac{Q_b(r) - r}{N_0} \pi(n), n = 1,2,..,N_0,$$

где $r = \sum_{n=1}^{N_0} C(n)\pi(n)$, $\pi(n) \in \pm 1$, $Q_b(\cdot)$ – равномерный квантователь с интервалом Δ, когда при *b*=0 и *b*=1 берутся чередующиеся точки. Упрощенная схема квантователя приведена на рисунке 1. На вход квантователя поступают значения *b* и *r*, при этом, если *b* = 1, на выходе квантователя будет ближайшее к *r* значение черной точки, если *b* = 0 – ближайшее к *r* значение белой точки.

Схема вложения информации методом QPD показана на рисунке 2 [5].

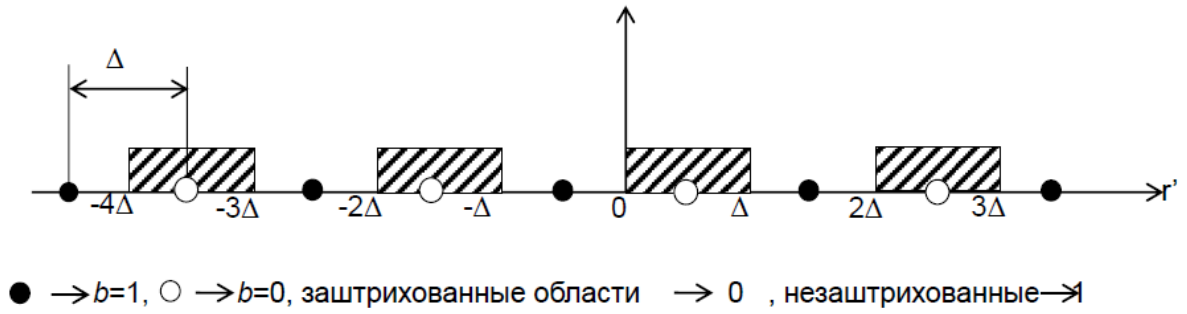

Рис. 1. Равномерный квантователь с шагом *Δ*

Извлечение информации выполняется слепым декодером по правилу:

$$\tilde{b} = \underset{b \in \{0,1\}}{\operatorname{argmin}} \|r' - Q_b(r)\|^2,$$

где $r' = \sum_{n=1}^{N_0} C'_w(n)\pi(n)$, $C'_w = C(n) + \varepsilon(n)$, $\varepsilon(n)$ – шум аддитивной атаки.

Вероятность ошибки при извлечении:

$$P = 2Q\left(\sqrt{\frac{0{,}75N_0}{\eta - 1}}\right).$$

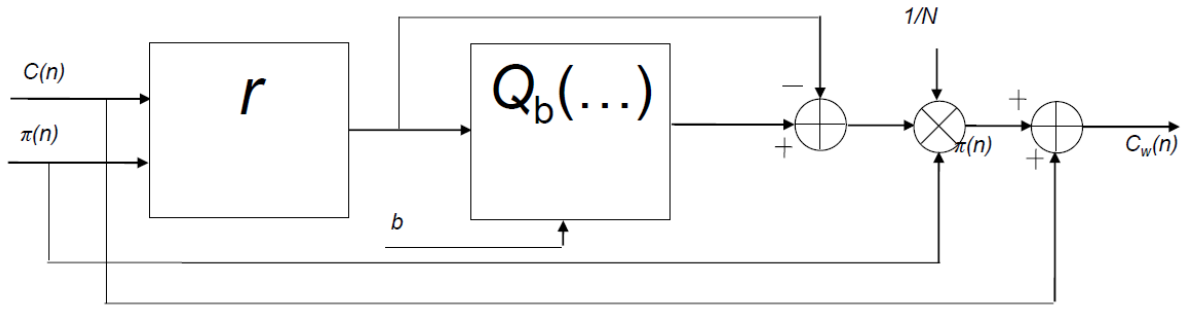

Рис. 2. Схема погружения для QPD

На рисунке 3 представлен график зависимости вероятности ошибки извлечения от отношения сигнал/шум после вложения (*Document to Watermark Ratio* – DWR), из которого видно, что ISS незначительно опережает QPD по данному показателю только при значении N_0, в несколько раз превышающем DWR. На рисунках 4 и 5 изображены графики зависимостей вероятности ошибки от отношения сигнал/шум после атаки (*Watermark to Noise Ratio* – WNR) и от значения величины N_0.

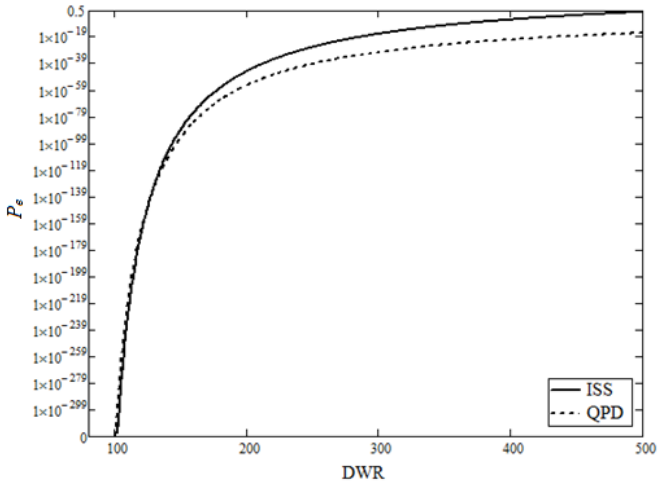

Рис. 3. Зависимость вероятности ошибки от отношения сигнал/шум после вложения, N_0 = 500, отношение сигнал/шум после атаки 80

Из рисунков 4–5 следует, что QPD превосходит ISS на несколько порядков при значениях N_0, не сильно превышающих DWR, однако при N_0 = 4DWR и более, ISS превосходит QPD по качеству извлечения. Тем не менее, стоит отметить, что увеличение N_0 приводит к снижению скорости вложения, поэтому при оптимальных значениях данного параметра QPD оказывается лучше.

Обнаружение стегосистемы. Пусть z – сигнал на входе детектора, событию H_0 соответствует случай, когда вложения в сигнале нет, событию H_1 – вложение есть. Детектор принимает решение M, при этом M = 1, если вложение найдено,

$M = 0$, если нет. Критериями эффективности обнаружения СГС являются вероятность пропуска СГС $P_m = P(M = 0|H_1)$ и вероятность ложного обнаружения СГС $P_{fa} = P(M = 1|H_0)$. Возможные соотношения между ними выражаются с помощью ROC-кривых [6]. Качество ROC-кривой может быть оценено при помощи ρ – надежности обнаружения, $\rho = 2A - 1$, где A – площадь под ROC-кривой.

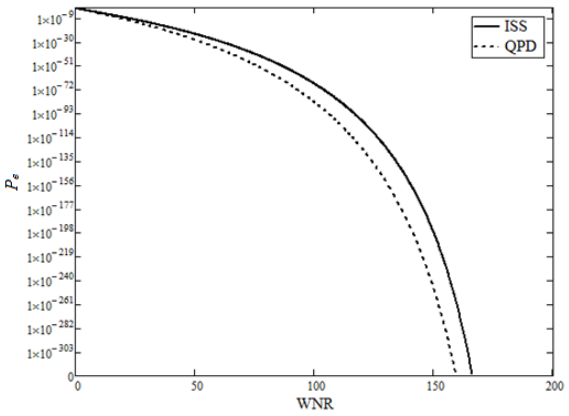

Рис. 4. Зависимость вероятности ошибки от отношения сигнал/шум после атаки. N_0 = 500, отношение сигнал/шум после вложения 200

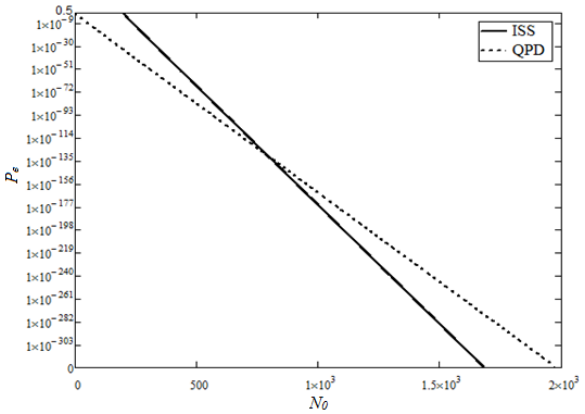

Рис. 5. Зависимость вероятности ошибки от N_0 (1..2000), отношение сигнал/шум после вложения 200, отношение сигнал/шум после атаки 100

Из графика на рисунке 6 видно, что площадь под ROC-кривыми для QPD при разных значениях N_0 меньше, чем для ISS. Это говорит о том, что при прочих равных условиях QPD обнаруживается хуже.

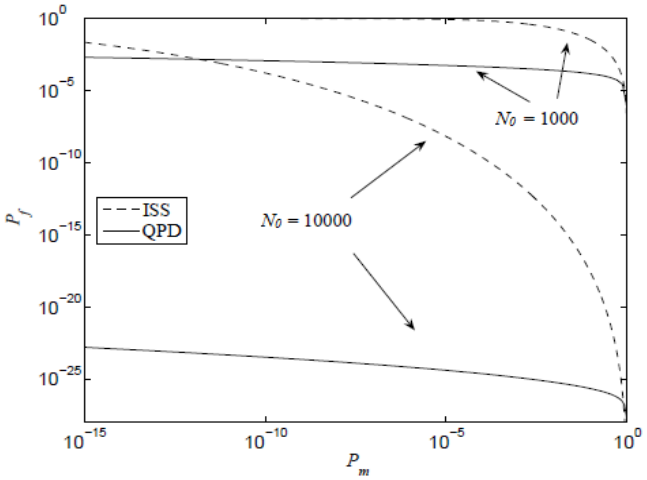

Рис. 6. ROC-кривые для ISS и QPD. Отношение сигнал/шум после вложения 200, отношение сигнал/шум после атаки 100

Таким образом, можно сделать вывод, что использование QPD является оптимальным, так как на практике для обеспечения приемлемой скорости вложения применяются не очень большие значения N_0, при которых QPD опережает ISS по всем параметрам.

Список используемых источников

1. Korzhik V., Morales Luna G., Loban K. Stegosystem Based on Noisy Channels // International Journal of Computer Science and Applications. 2011. Vol. 8 №. 1. P. 1–13.

2. Коржик В. И., Небаева К. А., Алексеевс М. Использование модели канала с шумом для построения стегосистемы // Телекоммуникации. 2013. S 7. С. 33–36.

3. Коржик В. И., Небаева К. А., Алексеевс М., Стегосистема для каналов с шумом при использовании «слепого» декодера // Международная научно-техническая и научно-методическая конференция «Актуальные проблемы инфотелекоммуникаций в науке и образовании». 20–24 февраля 2012: материалы конф., СПб., 2012. С. 238–240.

4. Небаева К. А. Стегосистемы на основе каналов с шумом при использовании слепого декодера // В мире научных открытий. 2013. № 10.1 (46). С. 118–132.

5. Небаева К. А. Разработка необнаруживаемых стегосистем для каналов с шумом : дис. … канд. техн. наук: 05.12.13 / Небаева Ксения Андреевна. СПб., 2014. 176 с.

6. Герлинг Е. Ю. Исследование и разработка методов обнаружения стеговложений в неподвижных изображениях : дис. … канд. техн. наук: 05.12.13 / Герлинг Екатерина Юрьевна. СПб., 2014. 211 с.

ИСПОЛЬЗОВАНИЕ МЕТОДА 3-БИТНОГО КВАНТОВАНИЯ ДЛЯ АЛГОРИТМА СЕЛЕКТИВНОЙ АУТЕНТИФИКАЦИИ ИЗОБРАЖЕНИЙ, УСТОЙЧИВОГО К JPEG СЖАТИЮ

А.Г. Жувикин, В.И. Коржик

Преимуществом использования цифровых водяных знаков является то, что они не требуют использования дополнительного объёма памяти для хранения метаданных. Однако, применение JPEG сжатия, как наиболее распространённого метода уменьшения размера изображений, приводит к нарушению целостности при использовании точной аутентификации. В данной работе предложен улучшенный метод селективной аутентификации изображений, устойчивый к JPEG сжатию, основанный на применении центральных конечных разностей и алгоритма 3-битного квантования вектора свойств. Экспериментальные результаты показали высокую устойчивость к JPEG сжатию с параметром качества $Q \geq 8$, высокую вероятность обнаружения искажений небольших искажений изображений, показатели $PSNR \geq 40$ дБ после погружения цифровых водяных знаков и низкую вычислительную сложность алгоритма по сравнению с предыдущим методам.

Ключевые слова: цифровые изображения; селективная аутентификация; JPEG; 3-битное квантование; вейвлет-преобразование Хаара; центральные конечные разности

THE USAGE OF 3-BIT QUANTIZATION METHOD FOR SELECTIVE IMAGE AUTHENTICATION ALGORITHM ROBUST TO JPEG COMPRESSION

Zhuvikin A., Korzhik V.

The advantage of watermarking usage is it does not require to store of metadata in extra memory space. However, JPEG algorithm, being a common method for image compression, leads to break-in of strict image authentication. An improved algorithm of selective image authentication tolerant to JPEG compression is presented. Proposed method is based on central finite differences