operational continuity management // Firs edition 2007-12-01. – 31 S.

17 Богуш В.М., Юдін О.К. Інформаційна безпека держави. - К.: МК-Прес, 2005 – 432 с.

18 Кононович В.Г., Тардаскін М.Ф. Основні положення концепції інформаційної безпеки телекомунікаційних мереж загального користування // Захист інформації, № 1, 2006. – 18-30 с.

19 Френцис Фукуяма. Великий крах. Людська природа і відновлення соціального порядку. Пер. З англ. В. Дмитрука. – Львів: Кальварія, 2005. – 380 с.

20 Фукуяма Ф. Наше постчеловеческое будущее. Последствия биотехнологической революции. – М.: АСТ, ЛЮКС, 2004. – 349 с.

21 Калашников М., Русов Р. Сверхчеловек говорит по-русски. Историко-футуристическое расследование. – М.: АСТ. Астрель, 2006. – 639 с.

УДК 519.688

А.В.Шишкин

ЭФФЕКТИВНАЯ СТЕГАНОГРАФИЧЕСКАЯ ПЕРЕДАЧА ИНФОРМАЦИИ В КОЭФФИЦИЕНТАХ ДИСКРЕТНОГО КОСИНУСНОГО ПРЕОБРАЗОВАНИЯ ПОЛУТОНОВЫХ ИЗОБРАЖЕНИЙ

Цифровая стеганография в настоящее время применяется в следующих технических задачах: защита информации от несанкционированного копирования путем встраивания цифровых водяных знаков (ЦВЗ) в информационный продукт (звук, изображение, видео); аутентификация информации; мониторинг радиопередач; скрытая передача информации в специальных приложениях и другие. Привлекательность стеганографии состоит в том, что она не требует каких-либо дополнительных ресурсов (объема памяти, расширения объема канала передачи), а использует имеющийся основной (или открытый) канал связи. Вопросам стеганографии посвящены отечественные и зарубежные монографии [1-3].

Совместно с криптографическими методами стеганография позволяет более эффективно решать задачи защиты информации. При этом встроенные ЦВЗ могут обеспечивать свои функции в течение всего времени использования информационного продукта, в то время как однажды взломанная криптосистема утрачивает в дальнейшем свои защитные свойства.

Стеганографическая система характеризуется следующими основными параметрами: вносимыми искажениями (distortions), удельным количеством скрываемой информации (или скоростью) (rate), устойчивостью (robustness) к различного рода помехам – атакам в канале передачи.

Под вносимыми искажениями понимают отличия стегосигнала, т.е. сигнала-носителя с встроенными ЦВЗ от исходного сигнала-носителя (или пустого контейнера). Встраивание ЦВЗ в сигнал-носитель неизбежно приводит к возникновению искажений последнего. В монографии [1] систематизированы всевозможные числовые оценки вносимых искажений. Наиболее распространенной мерой искажений является среднеквадратическая ошибка (СКО).

Удельное количество встроенной информации определяется средним количеством информации на один отсчет сигнала-носителя и измеряется соответственно в бит/отсчет.

Под устойчивостью понимают способность ЦВЗ противостоять различного рода непреодолимым и преднамеренным преобразованиям сигнала (атакам) в канале передачи: аналого-цифровому преобразованию, шумам, операциям сжатия, изменениям масштаба и др.

Указанные параметры – вносимые искажения, количество (скорость), устойчивость – взаимосвязаны. Нельзя одновременно улучшать все три параметра. Исходя из конкретных

требований к стегосистеме, задача состоит в нахождении компромисса между всеми этими параметрами.

ЦВЗ могут встраиваться как непосредственно в пиксели изображения, так и коэффициенты какого-либо преобразования исходного изображения. В данной работе решен вопрос выбора коэффициентов ДКП2 при сжатии изображений в соответствии со стандартной JPEG процедурой.

Исследуемая стеганографическая система представлена на рис. 1 в виде системы связи, использующей дополнительную информацию о состоянии канала на передающей стороне. Для встраивания информации d будем использовать коэффициенты двумерного дискретного косинусного преобразования исходного полутонового изображения. Использование преобразования исходного изображения позволяет равномерно распределить энергию встраиваемого сигнала равномерно по всему изображению, обеспечивая тем самым дополнительную визуальную невосприимчивость ЦВЗ. Для передачи коэффициентов со встроенными данными используется обратное двумерное ДКП (ОДКП2).

Рис. 1. Стеганографическая система передачи информации

Сигнал-носитель x в скрытом канале передачи является помехой для передаваемых данных d. Дополнительная помеха n, порождаемая JPEG сжатием, вносится в открытом канале передачи. Будем считать, что сигнал x доступен для кодера на передающей стороне. Если в кодере используется информация о сигнале-носителе, то кодер считается информированным; в противном случае кодер является неинформированным. Полагаем, что в декодере сигнал-носитель недоступен – это вариант неинформированного декодера (в англоязычной литературе для обозначения этого варианта декодера используется термин blind – "слепое" декодирование).

При условии, что сигнал-носитель x и шум n в открытом канале представляют собой процессы вида белого гауссовского шума $x \sim N(0, \sigma_x^2)$, $n \sim N(0, \sigma_n^2)$, скрытая пропускная способность в бит/отсчет для неинформированного декодера задается формулой [2,3]:

$$C = \frac{1}{2}\log_2\left(1 + \frac{\sigma_w^2}{\sigma_x^2 + \sigma_n^2}\right), \qquad (1)$$

где σ_w^2, σ_x^2, σ_n^2 – мощности сигнала ЦВЗ w, сигнала-носителя x и шума n в открытом канале соответственно.

Ясно, что для визуальной невосприимчивости встроенного сигнала w необходимо значительное превышение мощности сигнала-носителя над мощностью сигнала ЦВЗ: $\sigma_x^2 >> \sigma_w^2$. Если не учитывать в кодере сигнал-носитель, то в соответствии с формулой (1) рассчитывать на большой объем встроенной информации не приходится.

Однако, как показано в работе [4], использование информации о сигнале-носителе на передающей стороне позволяет теоретически исключить мешающее влияние последнего на передачу скрываемого сигнала. Для стеганографического канала передачи информации сигнал-носитель отражает состояние скрытого канала передачи и его пропускная способность определяется следующей формулой [5]:

$$C = \frac{1}{2}\log_2\left(1+\frac{\sigma_w^2}{\sigma_n^2}\right). \qquad (2)$$

В сравнении с формулой (1) пропускная способность скрытого канала передачи при учете сигнала-носителя значительно увеличивается. Соответственно, практически лучшие результаты по скорости (или объему) скрытой информации могут быть получены для информированного кодера. При этом декодер остается неинформированным.

Как следует из формулы (2), пропускная способность скрытого канала не зависит от самого сигнала-носителя, а определяется только отношением σ_w^2/σ_n^2. Данный результат не является тривиальным, т.к. мощность сигнала-носителя не входит в формулу (2) и, следовательно, сигнал x не оказывает никакого мешающего влияния на передачу скрываемого сигнала w.

Одним из практических способов использования дополнительной информации, позволяющим реализовать в значительной мере пропускную способность скрытого канала по формуле (2), является квантование передаваемых отсчетов во временной или частотной областях. В работе [6] такой способ назван модуляцией индекса квантования (МИК). В работе [7] исследован алгоритм МИК для канала с аддитивным белым гауссовским шумом.

При МИК отсчеты стегосигнала $s = x + w$ заменяют квантованными значениями сигнала-носителя: $s = q(x,\Delta,d)$ с учетом передаваемых данных. Функция квантователя при этом определяется следующей формулой:

$$q(x,\Delta,d) = \Delta\, round\left(\frac{x-\Delta d/4}{\Delta}\right)+\Delta d/4, \qquad (3)$$

где $d=(-1,1)$ - встраиваемые данные, Δ - шаг квантования, $round(.)$ - операция округления до ближайшего целого числа.

Полагаем, что сигнал-носитель x может принимать любые значения из области определения. Стегосигнал s принимает дискретные значения в зависимости от встраиваемого бита данных ЦВЗ. Сигнал ЦВЗ представляется соотношением:

$$w = q(x,\Delta,d) - x. \qquad (4)$$

Декодирование принимаемого сигнала $y = s + n$ осуществляется в соответствии с функцией:

$$\hat{d} = \arg\min_{d} |q(y,\Delta,d) - y|.$$

Операция $\arg\min_{x} f(x)$ обозначает нахождение значения x, для которого достигается минимальное значение функции $f(x)$ для всех возможных аргументов x.

В алгоритме (3) в один отсчет сигнала-носителя встраивается один бит информации. В алгоритме МИК с расширенным преобразованием (РП) [5] один бит встраиваемого ЦВЗ распределяется на L отсчетов носителя. В векторной форме стегосигнал представляется следующим образом:

$$\mathbf{s} = \mathbf{x} + \mathbf{w}, \qquad (5)$$

где $\mathbf{s}=(s_1, s_2,\ldots s_L)$, $\mathbf{x}=(x_1, x_2,\ldots x_L)$, $\mathbf{w}=(w_1, w_2,\ldots w_L)$ - векторы-строки длиной L соответственно стегосигнала, носителя и сигнала ЦВЗ.

Умножим обе части (5) справа на транспонированный вектор отсчетов двоичной случайной последовательности $\mathbf{u}=(u_1, u_2,\ldots u_L)$, $u_i=(-1,1)$:

$$\mathbf{su}' = \mathbf{xu}' + \mathbf{wu}'.$$

Далее получим:

$$\mathbf{wu}' = \tilde{s} - \tilde{x},$$

где $\tilde{s} = \mathbf{su}'$, $\tilde{x} = \mathbf{xu}'$ - скалярные величины.

Заменяя $\tilde{s}$ на квантованное значение в соответствии с функцией квантователя (3) $q(\tilde{x}, \Delta, d)$ и учитывая, что $\mathbf{uu}' = L$, получим выражение для вектора ЦВЗ в виде:

$$\mathbf{w} = \left(q(\tilde{x}, \Delta, d) - \tilde{x}\right)\mathbf{u}/L. \qquad (6)$$

Декодирование сигнала в алгоритме МИК-РП осуществляется в соответствии с функцией:

$$\hat{d} = \arg\min_{d} \left| q(\tilde{y}, \Delta, d) - \tilde{y} \right|,$$

где $\tilde{y} = \mathbf{yu}'$.

Случайный вектор $\mathbf{u}$ обеспечивает секретность ЦВЗ и затрудняет его обнаружение и декодирование без знания ключа.

Для эффективной стеганографической системы необходимо компромиссное решение задачи искажения-скорость-устойчивость. Определим шаг квантования через параметры стегосистемы, который позволяет эффективно решить указанный компромисс.

Принимая распределение сигнала ЦВЗ w в формуле (4) равномерным на интервале $(-\Delta/2, \Delta/2)$, получим значение для дисперсии:

$$\sigma_w^2 = \frac{1}{\Delta}\int_{-\Delta/2}^{\Delta/2} w^2 \, \mathrm{d}w = \frac{\Delta^2}{12L^2}.$$

Если встраиваются K бит информации, причем каждый бит распределяется на L коэффициентов ДКП2, то общее число модифицируемых коэффициентов составит значение $p = KL$. При этом полная энергия встроенного сигнала будет равна:

$$E_w = \sigma_w^2 KL = \frac{\Delta^2 K}{12L}. \qquad (7)$$

С другой стороны энергия $(m \times n)$-пиксельного полутонового изображения-носителя составит $E_x = \sigma_x^2 mn$. Здесь полная энергия изображения вычисляется по формуле:

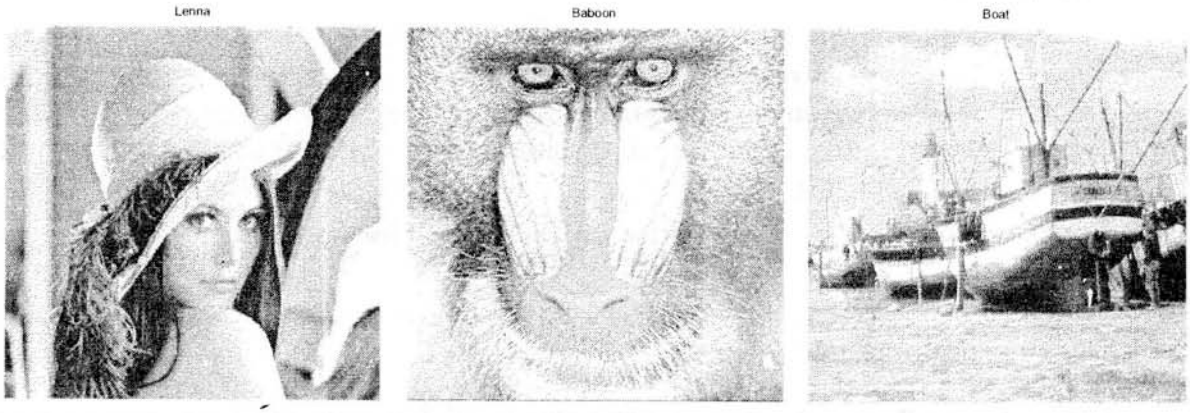
$$E_x = \sum_{i=1}^{m}\sum_{j=1}^{n} x_{ij}^2.$$

Если задать допустимое значение отношения мощности сигнала-носителя к мощности встроенного сигнала (Document-to-Watermark Ratio) в виде $DWR = E_x / E_w$, то, принимая во внимание равенство Парсеваля и учитывая (7), после очевидных преобразований, получим выражение для шага квантования:

$$\Delta = 2\sigma_x \sqrt{\frac{3mnL}{K \times DWR}}. \qquad (8)$$

Формула (8) позволяет рассчитать шаг квантования для алгоритма МИК-РП при известных характеристиках полутонового изображения σ_x, m, n, количестве встраиваемых бит информации K и коэффициенте DWR.

Важное значение имеет решение вопроса о выборе коэффициентов ДКП2, используемых для встраивания информации. Этот вопрос должен решаться с учетом характера ожидаемых преобразований в канале передачи изображения. Практически в настоящее время наиболее часто используется алгоритм JPEG DCT сжатия изображений [8]. Данный алгоритм относится к трансформирующему типу алгоритмов, для которых изображение первоначально разбивается на небольшие блоки, которые затем трансформируются в новое базисное пространство и квантуются с шагом квантованием, определяемым требуемым качеством (степенью сжатия). Результат квантования затем подвергается энтропийному кодированию для устранения избыточности. В стандартной процедуре JPEG сжатия формируют блоки размером 8x8 пикселей и в качестве преобразования используют двумерное ДКП. В зависимости от требуемого качества Q для



а) б) в)

Рис. 2. Полутоновые изображения размером 512x512, использованные для встраивания информации: а) Lenna; б) Baboon; в) Boat

сжатого изображения в каждом блоке используют не все 64 коэффициента, а меньшее их количество. При наименьшем качестве $Q=1$ передается только один коэффициент (постоянная составляющая), а при повышении качества используется большее число коэффициентов, количество которых также зависит от характера анализируемого блока. Максимальный коэффициент качества (минимальное сжатие) $Q=100$.

Процедуру JPEG сжатия можно рассматривать как канал связи с аддитивным шумом, поскольку операция квантования неизбежно приводит к появлению шумов квантования. При этом операции дискретного косинусного преобразования и энтропийного кодирования являются обратимыми и не влияют на передачу изображения-носителя и ЦВЗ.

В нашем случае максимальное количество коэффициентов ДКП2 для встраивания данных равно $m \times n$. Однако не все коэффициенты в равной степени пригодны для переноса скрытой информации. В результате JPEG сжатия низкочастотные коэффициенты, находящиеся в левом верхнем углу матрицы коэффициентов квантуются с меньшим шагом, нежели высокочастотные, расположенные в нижнем правом углу матрицы. В результате этого низкочастотные коэффициенты подвержены меньшему шуму, чем высокочастотные и для встраивания скрытой информации в первую очередь следует использовать именно их.

Для количественной оценки расстояния (i, j)-го коэффициента от матричного начала координат (1,1) будем использовать октаэдрическую (или единичную) норму и евклидову (квадратичную) нормы:

$$L_1 = (i-1)+(j-1). \qquad (9)$$

$$L_2 = \sqrt{(i-1)^2+(j-1)^2}\,. \qquad (10)$$

Норма L_1 соответствует направлению обхода матрицы в виде «зигзага», а евклидова норма L_2 соответствует обходу по «дуге». Расположим коэффициенты ДКП2 в порядке неубывания расстояния коэффициента от матричного начала координат и для встраивания данных будем использования первые KL коэффициентов, исключая нулевую составляющую.

В качестве сигнала-носителя x использовались 512×512 полутоновые изображения, традиционно применяемые в стеганографическом сообществе, - Lenna, Baboon, Boat (рис. 2). В качестве скрываемых данных d принималось черно-белое изображение в виде многократно повторяемой латинской буквы "G". Встраивание информации осуществляется по формуле (6) в коэффициенты ДКП2 размером 512×512. Последовательность коэффициентов формировалась в порядке неубывания их расстояния в метриках L_1 и L_2.

На рис. 3 представлены результаты декодирования скрываемого сигнала при JPEG сжатии изображения "Baboon" с встроенным черно-белым изображением в виде многократно

повторяемой латинской буквы "G" и использовании метрики L_1 для отбора коэффициентов при следующих условиях: коэффициенты качества Q=100, 75, 50 и 25; удельное количестве встроенной информации $R = 1/2$ бит/отсчет, коэффициент распределения $L = 1$; отношение $DWR = 30$ дБ. Для данного отношения DWR встроенные ЦВЗ визуально не обнаруживаются.

При наименьшем сжатии (Q=100) все скрываемые данные декодированы без ошибок. При увеличении степени сжатия (Q=75 и Q=50) возникают ошибки декодирования, причем вероятность ошибок увеличивается с увеличением расстояния коэффициентов-носителей от матричного начала координат. Для реализации удельного количества встроенной информации $R = 1/2$ бит/отсчет использовалась ровно половина из всего количества коэффициентов. Экспериментально установлено, что выбор метрики для отбора коэффициентов практически не оказывает влияния на достоверность декодирования.

В таблице представлены значения коэффициентов качества Q, которые необходимы для достижения вероятности ошибки декодирования $p_e \le 10^{-5}$ при отношении $DWR = 30$ дБ и варьировании параметров R и L.

Таблица

Коэффициенты качества Q JPEG сжатия

R	1	1/2	1/4		1/16			1/64			1/256		
L	1	1	1	4	1	4	8	1	4	8	1	4	8
Q	98	95	90	97	50	80	90	25	25	25	15	15	18

При уменьшении количества встраиваемой информации повышается устойчивость скрытой информации к JPEG сжатию. Так, для $R = 1/256$ бит/отсчет (что соответствует 1024 скрытым битам информации в полутоновом изображении 512×512 пикселей) возможно сжатие с коэффициентом качества Q=15 при вероятности ошибки декодирования $p_e \le 10^{-5}$. Увеличение коэффициента L во всех случаях не является целесообразным в канале с сжатием, поскольку при этом требуется большее количество коэффициентов для переноса скрытой информации. В то же время возможный ресурс вносимых искажений в виде мощности σ_w^2 следует распределять на коэффициенты в низкочастотной области, наименее подверженные шумам в JPEG канале.

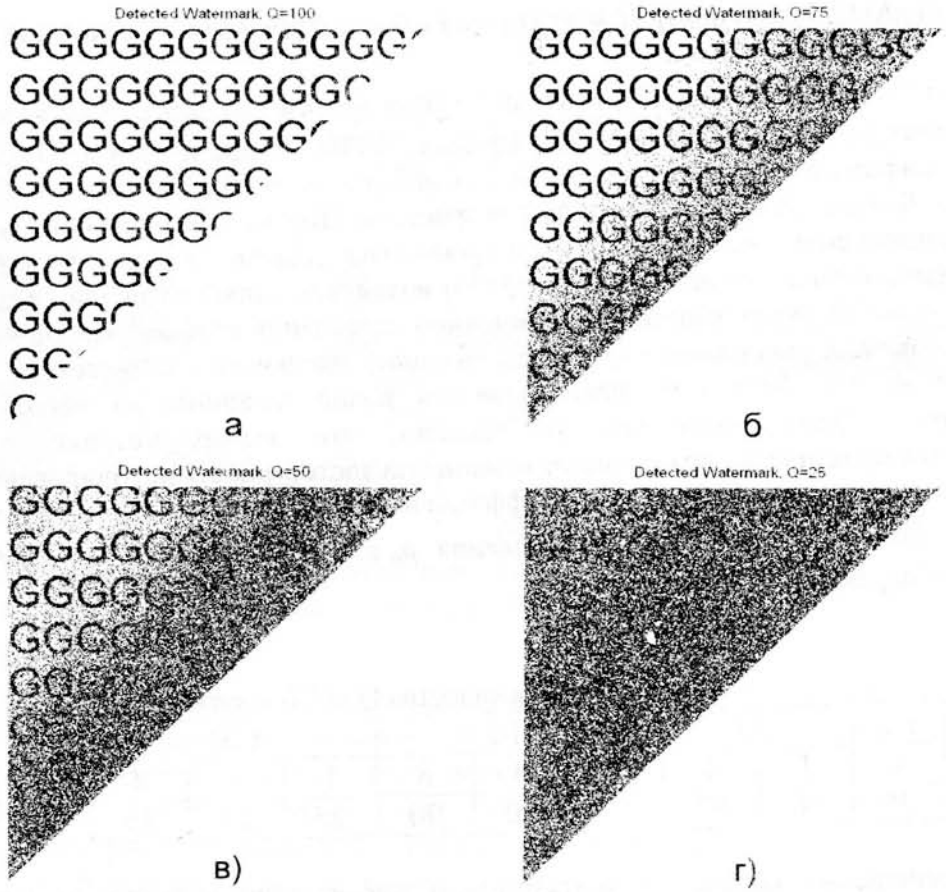


Рис. 3. Декодированная информация (буква "G") при JPEG сжатии с коэффициентами качества Q=100, 75, 50 и 25: а), б), в) и г) соответственно

Для встраивания ЦВЗ следует использовать наименее удаленные от матричного начала координат коэффициенты, используя для вычисления расстояния метрики (9) или (10).

Список литературы

1. *Конахович Г.Ф., Пузыренко А.Ю.* Компьютерная стеганография. Теория и практика. – К.: МК-Пресс, 2006. – 288 с.

2. *Грибунин В.Г., Оков И.Н., Туринцев И.В.* Цифровая стеганография. – М.: СОЛОН-Пресс, 2002. – 272 с.

3. *Cox I.J., Miller M.L., Bloom J.A.* Digital watermarking. – Morgan Kaufmann Publishers, 2002. – 542 p.

4. *Gel'fand S.I., Pinsker M.S.* Coding for channel with random parameters. // Problems of Control and Information Theory. – 1980. – 9, 1. – pp. 19-31.

5. *Costa M.H.M.* Writing on dirty paper, // IEEE Transactions on Information Theory. – 1983. – IT-29, pp. 439 - 441.

6. *Chen B., Wornell G.W.* Quantization index modulation: a class of provably good methods for digital watermarking and information embedding // IEEE Transactions on Information Theory. – 2001. 47, 4, pp. 1423 - 1443.

7. *Шишкин А.В., Кошевой В.М.* Устойчивая к атакам масштабирования стеганографическая передача информации с исключением мешающего влияния сигнала-носителя // Радиоэлектроника (Известия вузов). – 2007. – 50, 6. – сс. 3 – 15.

8. *Бондарев В.Н., Трёстер Г., Чернега В.С.* Цифровая обработка сигналов: методы и средства. Учеб. пособие для вузов. 2-е изд. – Х.: Конус, 2001. – 398 с.