УДК 004.056.5

**И.И. Бобок**,
**А.А. Кобозева**, д.т.н., профессор,
**Е.В. Малахов**, д.т.н., профессор,
**А.Д. Шовкун**

# МЕТОД ОРГАНИЗАЦИИ СКРЫТОГО КАНАЛА СВЯЗИ, ОБЕСПЕЧИВАЮЩИЙ ПРОВЕРКУ ЦЕЛОСТНОСТИ КОНТЕЙНЕРА

*Разработан стеганографический метод, позволяющий одновременно решать задачи скрытой передачи информации и проверки целостности контейнера. Приведены результаты вычислительного эксперимента.*

***Ключевые слова:*** *стеганографический алгоритм, контейнер, стеганосообщение, аутентификация.*

*Розроблено стеганографічний метод, що дозволяє одночасно вирішувати задачі прихованої передачі інформації й перевірки цілісності контейнера. Наведено результати обчислювального експерименту.*

***Ключові слова:*** *стеганографічний алгоритм, контейнер, стеганоповідомлення, аутентифікація.*

*Steganographic method for the solving of two problems - secure communication and authentication of the cover- is worked out. The results of computer experiments are stated.*

***Keywords:*** *steganographic algorithm, cover, stego message, authentication.*

В настоящее время общество вступает в такой период своего развития, который по праву можно назвать информационным. Информация становится одним из основных и самых дорогих товаров [1]. В силу этого большое внимание должно уделяться ее защите, в частности, реализации положений законодательства Украины об авторском праве.

Благодаря современным методам стеганографии [2–6] было сформировано одно из перспективных направлений защиты информации, которое позволяет в рамках традиционно существующих информационных потоков или информационной среды решать некоторые важные задачи информационной безопасности ряда прикладных областей [6–9].

Стеганографирование осуществляется различными способами [1, 4, 6]. Общей чертой этих способов является то, что скрываемое сообщение или дополнительная информация (ДИ), встраивается в некоторый не привлекающий внимание объект или контейнер. Процесс погружения ДИ в контейнер, или основное сообщение (ОС), будем называть стеганопреобразованием (СП), а результат СП – стеганосообщением (СС). Полученное СС затем пересылается адресату по открытому каналу связи или хранится в таком виде [6, 7].

В настоящее время активизировались исследования как в области “классической” стеганографии (проблемы, связанные с организацией секретного канала

внутри открытого канала связи), так и в области так называемых цифровых водяных знаков (ЦВЗ) – специальных "меток", внедряемых в изображение или другой сигнал с целью тем или иным образом контролировать его использование [7].

Технология ЦВЗ выступает в качестве эффективного решения проблемы защиты авторского права, позволяя идентифицировать источник, автора, владельца, дистрибьютора или уполномоченного потребителя цифровых изображений (ЦИ), видео- или звукозаписей, используется в основном для решения задачи аутентификации, доказательства целостности контента (в качестве ЦВЗ здесь часто выступают случайно сформированные бинарные последовательности). При внедрении ЦВЗ в информационный контент не всегда выдвигается требование обеспечения надежности восприятия получаемого СС [10]. При определенных условиях внедренный знак может (или должен) быть заметен. Это замечание существенно отличает методы, которые могут использоваться при решении задачи аутентификации, целостности, от методов решения другой стеганографической задачи – скрытой передачи данных. Однако если задача обеспечения надежности восприятия при внедрении ЦВЗ все-таки ставится, то принципиального противоречия для одновременного решения двух основных задач стеганографии – аутентификации и организации скрытой передачи информации – не возникает.

Проблема создания стеганографических методов для одновременного решения двух упомянутых выше задач уже рассматривалась в открытой печати, например, в [11, 12], однако предлагаемые здесь разработки имеют ряд существенных недостатков. Так алгоритм в [11] принципиально не может, если руководствоваться указанными в работе формулами для СП, обеспечить надежность восприятия СС для произвольного ЦИ-контейнера, хотя такая цель преследуется авторами, если используемый при СП коэффициент квантования $q$ будет больше единицы (что предполагается авторами). Также требует уточнений и обязательной корректировки, предложенный в [11] алгоритм декодирования ДИ.

В работе [12] индийскими учеными разработан стеганографический алгоритм для аутентификации и скрытой передачи данных, основанный на дискретном преобразовании Фурье. Но предложенный подход позволяет проводить аутентификацию только изображений в градациях серого, хранящихся в форматах TIFF и PNG, а секретное сообщение ограничено в размере, что сужает область применения алгоритма.

*Целью* исследования является разработка нового стеганографического метода, одновременно обеспечивающего аутентификацию сигнала-контейнера с соблюдением надежности восприятия СС и скрытую передачу произвольной информационной последовательности, устойчивого к возмущающим воздействиям, что позволит увеличить эффективность защиты секретной информации, передаваемой по открытому каналу связи.

Для достижения поставленной цели в работе решаются *задачи*:

1) разработки способа формирования ДИ таким образом, чтобы непосредственно погружаемое в ОС сообщение несло в себе наряду с передаваемой секретной информацией информацию для решения задачи аутентификации контейнера;

2) выбора размера секретного ключа, используемого для формирования ДИ, непосредственно погружаемой в ОС;

3) анализа работы и адаптации разработанного стеганографического метода путем обеспечения устойчивости соответствующих алгоритмов к возмущающим

воздействиям для возможности декодирования передаваемой ДИ в случае нарушения целостности сигнала, происходящего в результате применения атак (в частности, атаки сжатием).

Заметим, что моделирование неидеального канала связи в силу специфики рассматриваемой задачи имеет смысл проводить при помощи *малых* возмущающих воздействий [13], поскольку в результате любых атакующих воздействий на СС должна сохраняться его надежность восприятия, иначе действия противника будут без труда обнаружены сторонами, организующими секретный канал связи.

В качестве контейнера для простоты изложения в данной части работы используется монохромное ЦИ, $N \times N$ – матрицу которого обозначим $I$.

Далее будем различать ДИ и секретное сообщение (СРС): под СРС будем понимать информационное сообщение, передаваемое адресату, до процесса предварительного кодирования (рис. 2); под ДИ, как и ранее, понимается сообщение, которое непосредственно погружается в контейнер. ДИ формируется на основании СРС при помощи секретного ключа (рис. 2). В качестве СРС далее рассматривается случайно сформированная бинарная матрица соответствующего размера.

Пусть $K$ – бинарная $L \times L$-матрица ключа, используемого в процессе предварительного кодирования, $L$ – линейный размер квадратного блока матрицы изображения-контейнера, в который встраивается 1 бит ДИ; $W_b$ – $[N/L] \times [N/L]$ – матрица СРС, $\overline{W}_b$ – $N \times N$-матрица ДИ, $I'$ – $N \times N$-матрица СС.

Использование ключа при формировании ДИ из СРС обеспечит решение задачи 1 в перечне задач, приведенном выше.

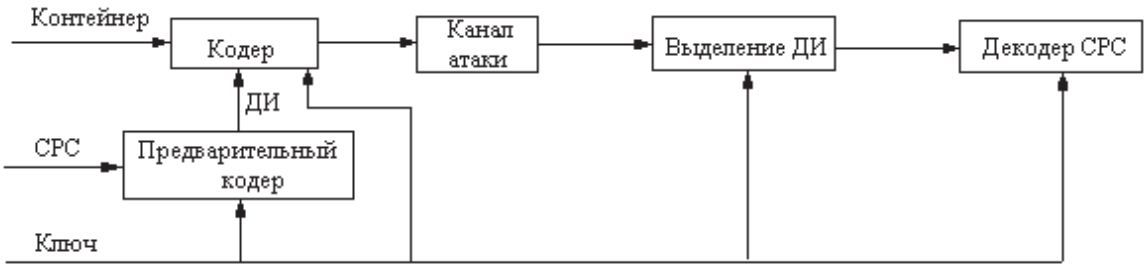


Рис. 2. Основные элементы используемой стеганосистемы

Работа прекодера (рис. 2) осуществляется в соответствии с формулой:

$$\overline{W}_b(n,m) = W_b\left(\left[\frac{n-1}{L}\right]+1, \left[\frac{m-1}{L}\right]+1\right) \oplus K(i,j), \quad n,m = 1,2,\ldots N,$$

где $$i = \begin{cases} L, \text{если} \quad \left\{\frac{n}{L}\right\} = 0, \\ \left\{\frac{n}{L}\right\}, \text{иначе} \end{cases}, \quad j = \begin{cases} L, \text{если} \quad \left\{\frac{m}{L}\right\} = 0, \\ \left\{\frac{m}{L}\right\}, \text{иначе} \end{cases},$$

$[\cdot]$ – операция округления до меньшего целого, $\{\cdot\}$ – 0 остаток от деления, $\oplus$ – операция логического исключающего ИЛИ.

Процесс СП происходит следующим образом:

$$I'(n,m)=\begin{cases}\left[\dfrac{I(n,m)}{q}\right]q, \text{ если } \overline{W}_b(n,m)=0,\\ \\ \left[\dfrac{I(n,m)}{q}\right]q+\dfrac{q}{2}, \text{ если } \overline{W}_b(n,m)=1,\end{cases} \qquad n,m=1,2,...N \tag{1}$$

где $q$ – четное число. Для достижения поставленной цели и решения задачи 3 в перечне задач приведенном выше, выбор коэффициента $q$ должен удовлетворять двум условиям: обеспечивать надежность восприятия СС и устойчивость разрабатываемого стеганометода (и соответствующих стеганоалгоритмов) к малым возмущающим $q$ воздействиям. Для гарантированного обеспечения первого (второго) условия $q$ должно иметь как можно меньшее (большее) значение, хотя надежность восприятия СС, как показывает вычислительный эксперимент, для большого числа тестируемых ЦИ обеспечивалась при предложенном способе СП (1) и для значительных $q$ ($q>20$). Окончательный выбор рекомендуемых компромиссных значений для параметра $q$ делается на основании представительного вычислительного эксперимента, результаты которого приведены ниже.

Процесс декодирования СРС выполняются следующим образом.

Обозначим $\overline{W_b'}$ – ДИ, полученную из СС, $W_b'$ – СРС, полученное из ДИ. Выделение ДИ производится в соответствии с формулой:

$$\overline{W_b'}(n,m)=\begin{cases}0, \quad \text{если} \quad \left\{\dfrac{I'(n,m)}{q}\right\}=0\\ \\ 1, \quad \text{если} \quad \left\{\dfrac{I'(n,m)}{q}\right\}=\dfrac{q}{2}\\ \\ \text{не определено}\end{cases} \qquad n,m=1,2,...N \tag{2}$$

Предположим, что декодирование согласно (2) завершилось определением всех бит ДИ. Это возможно в двух случаях: целостность ОС в ходе пересылки СС нарушена не была; целостность была нарушена активным (злоумышленным) нарушителем таким образом, что значения яркости всех пикселей в СС были оставлены либо кратными $q$, либо при делении на $q$ давали остаток $\dfrac{q}{2}$, но при этом порядок расположения пикселей с такими свойствами в СС нарушителем был изменен.

Для проверки аутентичности ОС и выделения из ДИ СРС необходимо произвести следующие действия. Для декодирования элемента матрицы СРС $W_b'(i,j)$, где $i,j=1,...,\left[\dfrac{N}{L}\right]$, выделяется соответствующий $L\times L$-блок матрицы $\overline{W_b'}$

ДИ, обозначаемый далее *B*, элементы которого определяются в соответствии с формулой:

$$B(m,l) = \overline{W_b}'\big((i-1)\cdot L + m, (j-1)\cdot L + l\big), \quad m,l = 1,\ldots, L. \tag{3}$$

Декодирование бита СРС производится следующим образом:

$$W_b'(i,j) = \begin{cases} 1, \textit{если} \quad B = \overline{K}, \\ 0, \textit{если} \quad B = K, \\ \textit{иначе не определен} \end{cases} \qquad i,j = 1,\ldots,\left[\frac{N}{L}\right],$$

где $\overline{K}$ – матрица, полученная из матрицы ключа К путем инвертирования.

Если при декодировании СРС все биты однозначно определены, то целостность контейнера нарушена не была. Неопределенность хотя бы одного бита $W_b'(i,j)$ говорит о нарушении целостности, причем это нарушение, практически достоверно, проведено активным (злонамеренным) нарушителем. Продолжение декодирования СРС в этом случае не имеет смысла.

Если при декодировании ДИ в соответствии с формулой (2) какой-либо бит не определится, то уже на этом этапе очевидно нарушение целостности. В силу того, что нарушение целостности могло произойти вследствие возмущающих воздействий, которые не являются действиями активного (злонамеренного) нарушителя, декодирование ДИ можно продолжить в соответствии с формулой:

$$\overline{W_b}'(n,m) = \begin{cases} 0, \textit{если}\left(\left\{\frac{I'(n,m)}{q}\right\} < q/2\right) AND(a < b) OR\left(\left\{\frac{I'(n,m)}{q}\right\} > q/2\right) AND(c < b) \\ 1, \textit{если}\left(\left\{\frac{I'(n,m)}{q}\right\} < q/2\right) AND(a \geq b) OR\left(\left\{\frac{I'(n,m)}{q}\right\} > q/2\right) AND(c \geq b) \end{cases} \quad n,m = 1,2,\ldots N$$

где $a = \left\{\frac{I'(n,m)}{q}\right\}$, $b = \left|\left\{\frac{I'(n,m)}{q}\right\} - q/2\right|$, $c = \left|\left\{\frac{I'(n,m)}{q}\right\} - q\right|$.

Если целостность была (непреднамеренно) нарушена, получение СРС выполняется следующим образом:

$$W_b'(i,j) = \begin{cases} 1, \textit{если} \quad \sum_{m,l=1}^{L}\left|B(m,l) - \overline{K}(m,l)\right| < \sum_{m,l=1}^{L}\left|B(m,l) - K(m,l)\right|, \\ 0, \textit{если} \quad \sum_{m,l=1}^{L}\left|B(m,l) - \overline{K}(m,l)\right| > \sum_{m,l=1}^{L}\left|B(m,l) - K(m,l)\right|, \\ \textit{иначе не определен} \end{cases} \qquad i,j = 1,\ldots,\left[\frac{N}{L}\right],$$

где $B$ определяется для элемента $W_b'(i, j), i, j = 1,...,\left[\frac{N}{L}\right]$ в соответствии с формулой (3).

***Замечание 1***. Эффективность защиты передаваемой информации в предложенном методе можно повысить. Выбор последовательности блоков ОС, в которые будет происходить погружение последовательных бит ДИ, можно производить в соответствии с дополнительным секретным ключом (рис. 2). В качестве такого ключа можно использовать, например, случайную перестановку натуральных чисел от 1 до $[N / L]\times[N / L]$, где $[N / L]\times[N / L]$ – это общее количество получаемых алгоритмом при СП блоков матрицы контейнера, в результате чего скрытая пропускная способность [7] организованного канала связи никак не пострадает.

***Результаты вычислительного эксперимента***

Для организации вычислительного эксперимента необходимо определить линейный размер $L$ квадратной матрицы секретного ключа $K$. Сложность выбора заключается в том, что, с одной стороны, чем больше $L$, тем выше защищенность передаваемой секретной информации; с другой стороны, чем больше $L$, тем меньше скрытая пропускная способность организуемого канала связи, поскольку $L\times L$-блок матрицы ОС используется для передачи одного бита ДИ. Разумный компромисс, как показывает практика, достигается при $L$=8.

Вычислительный эксперимент, в котором участвовало 200 ЦИ размером 800x800 пикселей, хранимых в различных форматах (с потерями, без потерь), проводился в среде Matlab. СРС представлялось бинарной $100\times100$-матрицей, в качестве ключа использовалась случайно сформированная бинарная $8\times8$-матрица $K$. В этой части эксперимента СС сохранялось в формате без потерь для исключения дополнительных возмущающих воздействий.

Надежность восприятия формируемого СС, оцениваемая путем субъективного ранжирования, обеспечивалась всегда при $q = 2,4,6,8$; для $q = 10,12$ обеспечивалась для подавляющего большинства протестированных ЦИ.

Эффективность декодирования СРС при тестировании работы предложенного стеганографического алгоритма определялась величиной объема восстановленной информации (ОВИ), который вычислялся в соответствии с формулой:

$$\frac{\left[\frac{N}{L}\right]^2 - \sum_{i,j=1}^{\left[\frac{N}{L}\right]} W_b(i, j) \oplus W_b'(i, j)}{\left[\frac{N}{L}\right]^2} \cdot 100\% .$$

В условиях отсутствия возмущающих воздействий на СС его аутентичность была подтверждена в 100 % тестируемых СС. ОВИ в этих условиях составил 100 %.

В условиях действий активного (злонамеренного) нарушителя, когда декодирование согласно (2) завершалось определением всех бит ДИ, фиксация нарушения аутентичности происходила в 100 % рассмотренных ЦИ.

Для дальнейшей проверки эффективности декодирования в условиях действий активного нарушителя искусственно создавалась ситуация нарушения целостности СС: оно подвергалось возмущающему воздействию, которое моделировалось путем наложения на СС гауссовского шума с нулевым математическим ожиданием и различными значениями дисперсии $d$ (такой способ моделирования активных атакующих действий, направленных на СС, является одним из традиционных [14]), а также мультипликативного шума, для чего в среде Matlab была использована процедура imnoise. Результаты экспериментов приведены в таблицах 1, 2 соответственно. Фиксация нарушения аутентичности происходила в 100 % тестируемых СС.

В результате проведенного эксперимента было установлено, что в качестве компромиссных значений параметра $q$ для удовлетворения требований обеспечения устойчивости разработанного алгоритма к возмущающим воздействиям наряду с надежностью восприятия формируемого им СС могут быть использованы $q = 8,10,12$ (табл. 1, 2).

*Таблица 1*

**Объем восстановленной информации из возмущенного путем наложения гауссовского шума стеганосообщения**

| | Среднее значение ОВИ для 200 тестируемых СС при различных значениях дисперсии $d$ (%) | | | | | Сохранение надежности восприятия СС |
|---|---|---|---|---|---|---|
| | $d = 0.0005$ | $d = 0.0001$ | $d = 0.00005$ | $d = 0.00001$ | $d = 0.000001$ | |
| $q = 4$ | 47,5 | 47,7 | 53,7 | 99,8 | 99,7 | + |
| $q = 6$ | 48,9 | 60,7 | 95,2 | 99,8 | 99,8 | + |
| $q = 8$ | 48,9 | 92,0 | 99,7 | 99,8 | 99,8 | + |
| $q = 10$ | 50,0 | 98,7 | 99,8 | 99,9 | 99,8 | ± |
| $q = 12$ | 53,6 | 98,7 | 99,9 | 99,9 | 99,9 | ± |
| $q = 14$ | 63,7 | 99,1 | 99,9 | 99,9 | 99,9 | ± |
| $q = 30$ | 99,2 | 99,5 | 99,9 | 99,9 | 99,9 | – |
| $q = 50$ | 99,3 | 99,5 | 99,9 | 100,0 | 100,0 | – |

*Таблица 2*

**Объем восстановленной информации из возмущенного путем наложения мультипликативного шума стеганосообщения**

| | Среднее значение ОВИ для 200 тестируемых СС при различных значениях дисперсии $d$ (%) | | | | | Сохранение надежности восприятия СС |
|---|---|---|---|---|---|---|
| | $d = 0.005$ | $d = 0.0005$ | $d = 0.0001$ | $d = 0.000001$ | $d = 0.0000001$ | |
| $q = 4$ | 42,8 | 52,9 | 60,2 | 63,4 | 99,8 | + |
| $q = 6$ | 51,9 | 58,6 | 85,7 | 85,7 | 99,8 | + |
| $q = 8$ | 54,2 | 56,5 | 91,7 | 97,4 | 99,7 | + |
| $q = 10$ | 53,0 | 66,5 | 98,7 | 99,8 | 99,8 | ± |
| $q = 12$ | 55,5 | 77,8 | 99,8 | 99,8 | 99,9 | ± |
| $q = 14$ | 55,2 | 87,4 | 99,6 | 99,2 | 99,9 | ± |
| $q = 30$ | 77,1 | 99,9 | 99,3 | 99,6 | 99,6 | – |
| $q = 50$ | 91,7 | 99,3 | 99,6 | 99,4 | 99,5 | – |

***Замечание 2***. В силу высокой эффективности декодирования алгоритма в условиях возмущающих воздействий для больших значений $q$ (табл. 1, 2) при СП можно использовать $q > 10$ с последующим наложением шума на СС для маскировки возможных нарушений надежности восприятия.

Для повышения устойчивости предложенного стеганографического метода к возмущающим воздействиям в качестве контейнера использовались цветные RGB-изображения [15]. Погружение одной и той же ДИ происходило в каждую (R, G и B) матрицу ОС. При этом для декодировании очередного бита СРС это значение выделялось трижды (из каждой составляющей R, G, B СС). Из полученной бинарной триады выбиралось в качестве итогового значения то, которое встречалось чаще. Результаты, сравнение которых с аналогичными результатами для монохромных ЦИ-контейнеров (табл. 1), приведенные в таблице 3, подтверждают повышение устойчивости разработанного метода к возмущающим воздействиям.

*Таблица 3*

**Объем восстановленной информации из возмущенного путем наложения гауссовского шума стеганосообщения, сформированного на основе RGB-контейнера**

| | Среднее значение ОВИ для 200 тестируемых СС при различных значениях дисперсии $d$ (%) | | | | | Сохранение надежности восприятия СС |
|---|---|---|---|---|---|---|
| | $d = 0.0005$ | $d = 0.0001$ | $d = 0.00005$ | $d = 0.00001$ | $d = 0.000001$ | |
| $q = 4$ | 63,9 | 71,4 | 53,7 | 86,6 | 99,6 | + |
| $q = 6$ | 67,1 | 76,4 | 95,2 | 99,3 | 99,9 | + |
| $q = 8$ | 69,6 | 89,0 | 99,7 | 99,5 | 99,5 | + |
| $q = 10$ | 68,3 | 99,7 | 99,8 | 98,7 | 99,8 | ± |
| $q = 12$ | 66,8 | 100,0 | 99,9 | 99,5 | 100,0 | ± |
| $q = 14$ | 76,5 | 98,6 | 99,9 | 100,0 | 98,9 | ± |
| $q = 30$ | 99,8 | 99,8 | 99,9 | 98,5 | 99,8 | – |
| $q = 50$ | 98,5 | 98,4 | 99,9 | 99,3 | 98,6 | – |

Использование RGB-контейнеров также позволяет практически в три раза повысить пропускную способность организуемого при помощи предложенного стеганографического метода канала скрытой связи [7]: погружение ДИ происходит последовательно в каждую из матрицы R, G и B ОС (при этом выбор порядка матриц R, G, B может быть частью секретного ключа).

Следующим этапом вычислительного эксперимента был анализ эффективности разработанного метода по отношению к атаке сжатием, являющейся в настоящий момент одной из наиболее часто используемых в стеганографии [4, 7]. Эксперимент был построен следующим образом. Использовался наиболее устойчивый к возмущающим воздействиям вариант разработанного метода: в каждую из матриц RGB-контейнера погружалась одна и та же ДИ, после чего СС сохранялось в формате без потерь (например, TIFF). Далее в среде Photoshop полученное СС пересохранялось в формате JPEG, с различными коэффициентами качества $Q$, после чего происходило декодирование СРС так, как описано выше. Результаты эксперимента приведены в таблице 4. Отметим, что хотя в таблице 4 для полноты эксперимента приведены результаты для $Q$=4.6, такие атаки на СС не рассматриваются как возможные на практике, поскольку не сохраняют

надежность восприятия СС [16]. С учетом этого, полученные результаты приводят к таким выводам: для $q \geq 16$ разработанный стеганоалгоритм является устойчивым к атаке сжатием ($Q \geq 8$), причем при $q$=16 в подавляющем большинстве тестируемых ЦИ надежность восприятия за счет наличия сжатия была обеспечена.

*Таблица 4*

**Объем восстановленной информации из стеганосообщения, сформированного в формате JPEG**

| | Среднее значение ОВИ для 200 тестируемых СС, сохраненных в JPEG с различными коэффициентами качества $Q$ (%) | | | | |
|---|---|---|---|---|---|
| | $Q=12$ | $Q=10$ | $Q=8$ | $Q=6$ | $Q=4$ |
| $q=4$ | 98,87 | 64,53 | 61,32 | 61,81 | 61,50 |
| $q=6$ | 100,00 | 63,11 | 46,60 | 48,69 | 47,10 |
| $q=8$ | 100,00 | 80,73 | 60,35 | 56,97 | 54,30 |
| $q=10$ | 100,00 | 88,75 | 62,34 | 56,23 | 49,01 |
| $q=16$ | 100,00 | 99,61 | 84,60 | 75,45 | 60,04 |
| $q=30$ | 100,00 | 100,00 | 100,00 | 93,01 | 82,49 |
| $q=50$ | 99,42 | 99,39 | 99,04 | 99,04 | 93,42 |
| $q=60$ | 100,00 | 100,00 | 100,00 | 98,88 | 97,03 |
| $q=70$ | 100,00 | 100,00 | 100,00 | 99,47 | 98,77 |

***Выводы***

В процессе работы был разработан новый стеганографический метод, позволяющий одновременно решать задачи скрытой передачи произвольной информационной последовательности и аутентификации контейнера, допускающий использование в качестве основного сообщения цифрового изображения, хранимого в произвольном формате.

При отсутствии возмущающих воздействий подтверждение аутентичности контейнера является достоверным событием. При наличии атакующих действий, направленных на стеганосообщение, нарушение аутентичности было зафиксировано в 100 % тестируемых информационных контентов.

Выбор параметра $q$, используемого при СП, позволяет:

– гарантировано обеспечить надежность восприятия стеганосообщения, определяемую путем субъективного ранжирования, при $q$=2,4,6,8;

– обеспечить ОВИ более 90 % при $q > 6$ в условиях возмущающих воздействий (нарушения целостности), что говорит об устойчивости разработанного стеганографического метода, в том числе и к атаке сжатием.

Внедрение ДИ в ОС при помощи (1) приводит к тому, что значения яркости каждого пикселя СС будет либо кратно $q$, либо при делении на $q$ давать остаток $\frac{q}{2}$. При $q > 2$ такая особенность будет зафиксирована практически достоверно любым пассивным нарушителем [7] даже без использования стеганоаналитических средств. В силу этого, можно порекомендовать воспользоваться предложением, высказанным в замечании 2, т.е. наложить на полученное СС шум. Однако если организованный канал скрытой передачи данных подвергается стеганоаналитическим проверкам, то наложение шума не спасает от его выявления

методом, предложенным в [17, 18]: 95 %–98 % СС детектировались как ЦИ, претерпевшие СП. Таким образом, устойчивость разработанного стеганографического метода к стеганоанализу остается пока нерешенной проблемой, над которой продолжают работать авторы.

## СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ


1. *Хорошко В.А.* Методы и средства защиты информации / В.А. Хорошко, А.А. Чекатков. – К. : Юниор, 2003. – 501 с.

2. *Корольов В.Ю.* Планування досліджень методів стеганографії та стеганоаналізу / В.Ю. Корольов, В.В. Поліновський, В.А. Герасименко, М.Л. Горінштейн // Вісник Хмельницького національного університету. – 2011. – № 4. – С. 187–196.

3. *Королев В.Ю.* Стеганография по методу наименее значимого бита на базе персонализированных флеш-накопителей / В.Ю. Королев, В.В. Полиновский, В.А. Герасименко // Управляющие системы и машины. – 2011. – № 1 (231). – С. 79–87.

4. *Аграновский А.В.* Стеганография, цифровые водяные знаки и стеганоанализ / А.В. Аграновский, А.В. Балакин, В.Г. Грибунин, С.А. Сапожников. – М. : Вузовская книга, 2009. – 220 с.

5. Advanced Statistical Steganalisis / R. Bohme, Springer, 2010.

6. *Кобозєва А.А.* Аналіз захищеності інформаційних систем / А.А. Кобозєва, І.О. Мачалін, В.О. Хорошко. – К. : Вид. ДУІКТ, 2010. – 316 с.

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

8. *Конахович Г.Ф.* Компьютерная стеганография. Теория и практика / Г.Ф. Конахович, А.Ю. Пузыренко. – К. : МК–Пресс, 2006.

9. *Карпинец В.В.* Решение проблемы уменьшения уровня искажений векторных изображений вследствие встраивания цифровых водяных знаков / В.В. Карпинец, Ю.Е. Яремчук // Информатика и математические методы в моделировании. – 2011. – Т. 1. – № 2. – С. 131–140.

10. *Кобозева А.А.* Учет свойств нормального спектрального разложения матрицы контейнера при обеспечении надежности восприятия стегосообщения / А.А. Кобозева, Е.А. Трифонова // Вестник НТУ "ХПИ". – 2007. – № 18. – С. 81–93.

11. *Глумов Н.И.* Алгоритм встраивания полухрупких цифровых водяных знаков для задач аутентификации изображений и скрытой передачи информации / Н.И. Глумов, В.А. Митекин // Компьютерная оптика. – 2011. – № 2. – Т. 35. – С. 262–267.

12. *Bhattacharyya D.* Authentication and Secret Message Transmission / D. Bhattacharyya, J. Dutta, P. Das, S.K. Bandyopadhyay, T. Kim // Int. J. Communications, Network and System Sciences. – 2009. – № 5. – P. 363–370.

13. *Кобозєва А.А.* Новий підхід до проблеми стеганоаналізу / А.А. Кобозєва // Інформатика та математичні методи в моделюванні. – 2011. – Т. 1. – № 2. – С. 183–189.

14. *Gkizeli M.* Optimal Signature Design for Spread-Spectrum Steganography / M. Gkizeli, D.A. Pados, M.J. Medley. – IEEE Trans. On Image Processing, vol.16, no.2, Feb. 2007.

15. *Гонсалес Р.* Цифровая обработка изображений / Р. Гонсалес, Р. Вудс ; пер. с англ. ; под ред. П.А. Чочиа. – М. : Техносфера, 2005. – 1072 с.

16. *Кобозева А.А.* Анализ особенностей сингулярных чисел матриц цифровых изображений при разных степенях сжатия для выявления фотомонтажа / А.А. Кобозева, В.В. Зорило // Захист інформації. – 2010. – № 3. – С. 34–41.

17. *Бобок И.И.* Стеганоаналитический метод для цифрового сигнала-контейнера, хранящегося в формате с потерями / И.И. Бобок // Сучасний захист інформації. – 2011. – № 2. – С. 50–60.

18. *Бобок И.И.* Детектирование наличия возмущений матрицы цифрового изображения как составная часть стеганоанализа / И.И. Бобок // Вісник Східноукр. нац. ун-ту ім. В. Даля. – 2011. – № 7 (161). – С. 32–41.


Отримано 20.04.2012