УДК 004.056.5

А.А. Кобозева,
доктор технических наук, профессор

МЕТОД СКРЫТОЙ ПЕРЕДАЧИ ДАННЫХ, ОБЕСПЕЧИВАЮЩИЙ АУТЕНТИФИКАЦИЮ КОНТЕЙНЕРА, ОСНОВАННЫЙ НА РЕШЕНИИ СИСТЕМ ЛИНЕЙНЫХ УРАВНЕНИЙ

Создан новый стеганографический метод, позволяющий одновременно решать задачи скрытой передачи информации и аутентификации контейнера, основанный на решении систем линейных уравнений.

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

Створено новий стеганографічний метод, що дозволяє одночасно вирішувати задачі прихованої передачі інформації й аутентифікації контейнера, заснований на рішенні систем лінійних рівнянь.

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

New steganographic algorithm, allowing simultaneously solving two problems – the problem of hidden data transfer and container authentication, based on the solving of the systems of linear equations is created.

Keywords: *steganographic algorithm, container, stegomessage, authentication.*

Стеганография – одно из наиболее древних [1] и одновременно наиболее перспективных современных направлений защиты информации [2–6], особенностью которого является то, что оно не предусматривает прямого оглашения факта существования защищаемой информации. В процессе стеганографирования скрываемое сообщение или дополнительная информация (ДИ) встраивается в непривлекающий внимание объект или контейнер, который затем передается по открытому каналу связи. В настоящий момент в качестве таких объектов часто используются цифровые сигналы: изображения (ЦИ), аудио, видео. Не ограничивая общности рассуждений, для простоты изложения далее как контейнер рассматривается ЦИ в градациях серого.

Поскольку современная цифровая стеганография является сравнительно молодой наукой [1], ее терминология еще не устоялась. Оговорим, что процесс погружения ДИ в контейнер, или основное сообщение (ОС), будем называть стеганопреобразованием (СП), а результат СП – стеганосообщением (СС).

В настоящее время интерес к стеганографическим методам значительно вырос. Для этого существуют две основные причины. Во-первых, это ограничение на использование криптосредств в ряде стран мира, в том числе в Украине; во-вторых, с ростом объема информации, представленной в цифровом виде, повысилась актуальность проблемы защиты прав собственности на такую инфор-

мацию [2, 6]. Логическим следствием здесь стала активизация исследований в двух основных направлениях: в области "классической" стеганографии (проблемы, связанные с организацией секретного канала внутри открытого канала связи); в области так называемых цифровых водяных знаков (ЦВЗ) – специальных "меток", внедряемых в сигнал с целью контроля его использования [7].

При внедрении ЦВЗ в информационный контент не всегда выдвигается требование обеспечения надежности восприятия получаемого СС [8]. При определенных условиях внедренный знак может (или должен) быть заметен. Это замечание существенно отличает методы, которые могут использоваться при решении задачи аутентификации, от методов решения 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, которые в совокупности будем называть *double*-задачей, не возникает.

Проблема создания стеганографических алгоритмов для решения *double*-задачи уже рассматривалась в открытой печати [9–11], однако предлагаемые здесь разработки имеют ряд существенных недостатков. Так алгоритм в [9] в большинстве случаев своего возможного использования не может обеспечить надежность восприятия СС для произвольного ЦИ-контейнера, хотя такая цель преследуется авторами. Алгоритм, предложенный в [10], формирует СС, чувствительное не только к преднамеренным, но и к непреднамеренным атакам, позволяет проводить аутентификацию только изображений в градациях серого, хранимых в форматах TIF и PNG. В [11] разработан алгоритм, свободный от двух недостатков упомянутых выше, но неустойчивый к стеганоанализу, осуществляемому экспертом даже без привлечения каких-либо специальных программных средств (назовем такой алгоритм тривиально неустойчивым к стеганоанализу): значения яркости каждого пикселя СС либо кратно некоторому заданному натуральному q, либо при делении на q дает остаток $\frac{q}{2}$.

Все вышесказанное подтверждает *актуальность* проблемы создания новых стеганографических алгоритмов и методов, решающих *double*-задачу.

Целью настоящей работы является разработка нового стеганографического метода для решения *double*-задачи, обеспечивающего надежность восприятия СС, применимого для цифрового изображения, хранимого в произвольном формате, не являющегося тривиально неустойчивым к стеганоанализу.

Для достижения поставленной цели необходимо решить *задачи*:

1. Организации процесса предварительного кодирования секретного сообщения таким образом, чтобы сформированная в результате ДИ несла в себе наряду с передаваемой секретной информацией информацию для решения задачи аутентификации контейнера;

2. Построения секретного ключа, используемого при предварительном кодировании секретного сообщения, а также при выделении из СС ДИ, таким образом, чтобы эти процессы были свободны от вычислительной погрешности;

3. Обеспечения возможности эффектиной работы разработанного метода в условиях неидеального канала связи с целью декодирования передаваемой секретной информации даже в случае нарушения аутентичности сигнала.

Основными математическими инструментами, используемыми в работе, являются матричный анализ [12] и теория относительных возмущений [13].

Обозначим $n \times m$-матрицу монохромного ЦИ, используемого в качестве контейнера F. Далее будем различать ДИ и секретное сообщение (СРС): под СРС будем понимать информационное сообщение, передаваемое адресату, до процесса предварительного кодирования (рис. 1); под ДИ, как и ранее, понимается сообщение, которое непосредственно погружается в контейнер. ДИ формируется на основании СРС при помощи секретного ключа (рис. 1). В качестве СРС далее рассматривается случайно сформированная бинарная последовательность $p_1, p_2,...,p_l$, элементы которой принадлежат множеству $\{-1,1\}$.

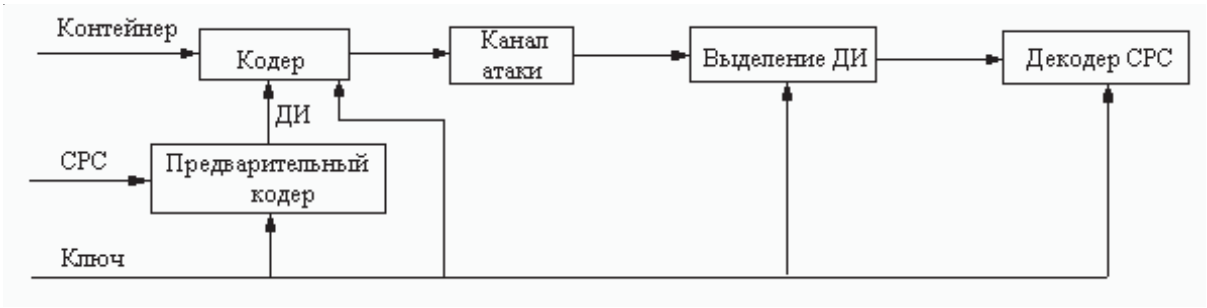

Рис. 1. Основные элементы используемой стеганосистемы

Основные шаги базового метода для погружения СРС выглядят следующим образом.

1. Матрица F разбивается на $r \times r$-блоки (будем обозначать произвольный $r \times r$-блок B). Каждый блок в базовом методе служит для погружения в него 1 бита СРС.

2. *Погружение*. Пусть B – очередной блок ОС с элементами $b_{ij}, i, j = \overline{1,r}$, в который погружается очередной бит СРС p_k. Для погружения необходимо выполнять следующие задачи:

2.1. Построение ключа. По матрице B строится нижняя треугольная $r \times r$-матрица L, элементы l_{il} которой определяются следующим образом:

$$l_{ij} = \begin{cases} 0, \textit{ если } i < j, \\ r, \textit{ если } i = j, \\ 0, \textit{ если } (i. > j) \,\&\, (b_{ij} < 127), \\ 1, \textit{ если } (i. > j) \,\&\, (b_{ij} \geq 127). \end{cases}$$

Матрица L используется для предварительного кодирования элементов СРС (рис. 1).

2.2. Предварительное кодирование. Элементу p_k СРС ставится в соответствие вектор x_P длины r по следующему правилу:

$$x_P = Lx,$$

где $x = (p_k, p_k, ..., p_k, p_k)^T$ – вектор длины r. Вектор x_P – составная часть ДИ, для которой выполняется ее непосредственное погружение в контейнер.

2.3. Погружение ДИ. Элементы вектора x_p погружаются в блок B в соответствии с выбранным предварительно стеганографическим алгоритмом. Результатом является блок стеганосообщения с матрицей $\overline{B}$. Погружение элемента p_k завершено.

Построение ключа – нижней треугольной матрицы – на шаге 2.1 может осуществляться различными способами. В частности, нижний треугольник такой матрицы может генерироваться случайным образом. Важным является лишь хорошая обусловленность этой матрицы, что гарантируется отсутствием нулей на главной диагонали.

Необходимо заметить, что элементы вектора x_p, получаемого на шаге 2.2, по модулю не превышают $2r-1$. Поэтому выбор размера блока r должен производиться так, чтобы даже при аддитивном погружении ДИ на шаге 2.3 надежность восприятия нарушена не была. В силу этого приемлемым здесь будет $r \le 8$ [14]. Вообще же надежность восприятия СС в предложенном методе обеспечивается выбранным для погружения вектора x_p стеганографическим алгоритмом и никак не ухудшается (улучшается) самим методом.

Пусть $\overline{F}$ – матрица анализируемого СС. Основные шаги алгоритма декодирования СРС и проверки аутентичности.

1. Матрица $\overline{F}$ разбивается на $r \times r$-блоки. Каждый блок $\overline{B}$ служит для извлечения из него 1 бита СРС.

2. Пусть $\overline{B}$ – очередной блок СС с элементами $\overline{b}_{ij}$, $i, j = \overline{1,r}$, из которого извлекается очередной бит СРС p_k. Для извлечения необходимо:

2.1. *Декодирование ДИ.* С учетом использованного при погружении ДИ стеганографического алгоритма из блока $\overline{B}$ СС при помощи соответствующего алгоритма извлекается ДИ – вектор $\overline{x}_P$.

2.2. *Построение ключа.* По матрице $\overline{B}$ строится нижняя треугольная $r \times r$-матрица $\overline{L}$, элементы $\overline{l}_{ij}$ которой определяются аналогично элементам матрицы L:

$$\overline{l}_{ij} = \begin{cases} 0, \textit{если } i < j, \\ r, \textit{если } i = j, \\ 0, \textit{если } (i. > j) \,\&\, (\overline{b}_{ij} < 127), \\ 1, \textit{если } (i. > j) \,\&\, (\overline{b}_{ij} \ge 127). \end{cases}$$

2.3. *Декодирование элемента СРС.* Для декодирования элемента p_k СРС решается относительно неизвестного вектора $\overline{x}$ система линейных алгебраических уравнений:

$$\overline{L}\,\overline{x} = \overline{x}_P. \qquad (1)$$

2.3.1. *Анализ.* Если все элементы полученного вектора $\overline{x}$ одинаковы и равны 1 или –1, то нарушения целостности ОС не произошло, при этом в первом

случае $p_k = 1$, во втором – $p_k = -1$. Если же не все элементы $\bar{x}$ одинаковы, или среди них имеются элементы, отличные от 1, −1, то целостность контейнера была нарушена.

2.3.2.*Декодирование элемента СРС в случае нарушения целостности контейнера*. Среди элементов вектора $\bar{x}$ определяем значение $\bar{x}_{\max}$, которое встречается с максимальной частотой. Тогда:

$$p_k = \begin{cases} 1, \textit{ если } \bar{x}_{\max} = 1, \\ -1, \textit{ если } \bar{x}_{\max} = -1, \\ \textit{не определено, если } \bar{x}_{\max} \notin \{-1,1\}. \end{cases}$$

Матрицы $\bar{L}$ и L являются невырожденными ($\det L = \prod_{i=1}^{r} l_{ij} \neq 0;\ \det \bar{L} = \prod_{i=1}^{r} \bar{l}_{ij} \neq 0$) и хорошо обусловленными. Действительно, это нижние треугольные матрицы с ненулевыми элементами на главной диагонали, что говорит о линейной независимости их строк (столбцов). Кроме того, поскольку матрицы имеют диагональное преобладание по построению, их число обусловленности Скила мало [15]. Это приводит к малой чувствительности к возмущающим воздействиям задачи декодирования СРС на шаге 2.3: даже наличие вычислительной погрешности при решении СЛАУ (1) не приведет к значительной погрешности результата $\bar{x}$ [15], что важно при декодировании элемента СРС в случае нарушения целостности контейнера.

Замечание 1. При построении ключей $\bar{L}$ и L элементы их главных диагоналей можно положить равными 1. Это, оставив матрицы невырожденными, хотя и увеличит их числа обусловленности, но оставит матрицы хорошо обусловленными: линейная независимость их строк (столбцов) очевидно присутствует в силу треугольного вида $\bar{L}$ и L и отсутствия нулей на главных диагоналях [13]. Главным преимуществом ключей такого вида будет отсутствие вычислительной погрешности на шаге 2.3 разработанного метода в процессе декодирования. Таким образом, накопление вычислительной погрешности в предложенном методе может происходить только при работе предварительно выбранных конкретных стеганографических алгоритмов на шагах 2.3 и 2.1 погружения и декодирования соответственно.

Замечание 2. На первый взгляд может показаться, что процесс предварительного кодирования СРС можно свести только к получению вектора $x = (p_k, p_k, ..., p_k, p_k)^T$ и его последующему погружению в блок ОС в качестве ДИ. Тогда о сохранении целостности будет свидетельствовать равенство всех элементов соответствующего вектора $\bar{x}$, получаемого при декодировании ДИ, либо единицам, либо −1. Но, учитывая, что решается не только задача проверки аутентичности, но и секретной передачи данных, такой вид ДИ может привести к очень чувствительному к возмущающим воздействиям СС (например, если будет осуществлено аддитивное погружение): достаточно изменить значения яркости соответствующего пикселя, использованного для погружения, всего на ± 1, чтобы погруженная информация была утеряна. Использование же для предварительного кодирования еще нижней треугольной матрицы L приводит к

тому, что СС, в каждый блок которого внедрен вектор Lx, будет менее чувствительным к ВВ. Действительно, если значения элементов вектора Lx возмутить на ± 1, это даст возможность восстановить вектор $x = (p_k, p_k, ..., p_k, p_k)^T$ более точно при решении СЛАУ, чем при непосредственном декодировании [14, 15].

Замечание 3. Предложенный метод можно использовать для произвольного изображения-контейнера. Его устойчивость не зависит ни от формата хранения ЦИ, ни от непосредственных свойств матрицы ЦИ, поскольку процесс декодирования происходит путем решения СЛАУ с хорошо обусловленными (по построению) матрицами.

Замечание 4. Очевидно, что устойчивость предлагаемого метода к стеганоанализу будет определяться соответствующей устойчивостью выбранного для погружения ДИ стеганографического алгоритма.

Очевидным недостатком метода является его малая скрытая пропускная способность [1]: $1/r^2$ бит/пикс. Легко достигается увеличение пропускной способности в 2 раза. Для простоты предположим, что r – четное. На шаге предварительного кодирования паре p_k, p_{k+1} СРС поставим в соответствие вектор x_p длины r по правилу $x_P = Lx$, где

$$x = \left(\underbrace{p_k, ..., p_k}_{\frac{r}{2}}, \underbrace{p_{k+1}, ..., p_{k+1}}_{\frac{r}{2}} \right)^T$$

Установление аутентичности ОС будет проводиться путем сравнения совпадений первых $\frac{r}{2}$ элементов вектора $\bar{x}$ и последующих $\frac{r}{2}$ элементов.

Выводы

В работе 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. Выбор конкретного стеганографического алгоритма на шаге 2.3 при погружении и шаге 2.1 при декодировании ДИ выделяет из разработанного метода конкретный алгоритм, решающий *double*-задачу. Надежность восприятия СС, формируемого методом, а также степень устойчивости к стеганоанализу определяется предварительно выбранным для использования стеганографическим алгоритмом.

Разработанный метод допускает отсутствие вычислительной погрешности в случае, если ошибки округления отсутствуют в выбранном стеганоалгоритме, используемом непосредственно для погружения и извлечения ДИ; позволяет решать задачу секретной передачи информации даже в случае установленного нарушения аутентичности (если, конечно, это нарушение не было проведено активным нарушителем с учетом характеристик используемого алгоритма).

Недостатком разработанного метода является все еще недостаточная скрытая пропускная способность: $2/r^2$ бит/пикс, на увеличения которой направлены в настоящий момент усилия автора. Конечно, можно было бы увеличить пропускную способность, поступив аналогично тому, как было предложено выше: на шаге предварительного кодирования последовательности $p_k, p_{k+1}, ..., p_{k+n-1}$ СРС,

состоящей из n элементов, внедряемых в один $r \times r$-блок, поставить в соответствие вектор $x_P = Lx$, где

$$x = \left(\underbrace{p_k, \ldots, p_k}_{\frac{r}{n}}, \underbrace{p_{k+1}, \ldots, p_{k+1}}_{\frac{r}{n}}, \ldots, \underbrace{p_{k+n-1}, \ldots, p_{k+n-1}}_{\frac{r}{n}} \right)^T$$

Однако здесь важным будет соотношение между величинами r и n: уменьшение значения отношения r/n очевидно отрицательно скажется на эффективности декодирования СРС при нарушении аутентичности. Поэтому необходим принципиально иной способ для решения задачи увеличения скрытой пропускной способности. Настоящая статья является первым шагом автора в разработке метода для решения *double*-задачи, основанного на свойствах систем линейных алгебраических уравнений, и носит теоретический характер. Результаты вычислительных экспериментов, тестирующих работу метода на практике, в настоящий момент готовятся к печати.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Грибунин В.Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. – М. : Солон-Пресс, 2002. – 272 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. Bohme R. 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. Маракова И.И. Повышение эффективности сокрытия информации для систем с зашумленными каналами связи / И.И. Маракова, А.А. Яковенко // Інформатика та математичні методи в моделюванні. – 2012. – № 1, Т. 2. – С. 5–17.

8. 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.

9. 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.

10. 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.

11. Бобок И.И. Метод организации скрытого канала связи, обеспечивающий проверку целостности контейнера / И.И. Бобок, А.А. Кобозева, Е.В. Малахов, А.Д. Шовкун // Сучасна спеціальна техніка. – 2012. – № 2. – С. 12–19.

12. Гантмахер Ф.Р. Теория матриц / Ф.Р. Гантмахер. – М. : Наука, 1988. – 552 с.

13. Деммель Дж. Вычислительная линейная алгебра / Дж. Деммель ; пер. с англ. Х.Д. Икрамова. – М. : Мир, 2001. – 430 с.

14. Кобозева А.А. Практическая реализация стеганографическог метода, основанного на решении системы линейных алгебраических уравнений / А.А. Кобозева, И.И. Борисенко // Праці УНДІРТ. – 2006. – № 3 (47). – С. 78–83.

15. Кобозева А.А. Стеганографический метод, основанный на решении системы линейных алгебраических уравнений / А.А. Кобозева, А.В. Коломийчук // Праці УНДІРТ. – 2006. – № 1 (45), 2(46). – С. 104–109.

Отримано 11.09.2012