УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol. 3 (2013), No. 2, pp. 169-178

СТЕГАНОГРАФИЧЕСКИЙ МЕТОД ДВУХЭТАПНОГО ДЕКОДИРОВАНИЯ, ОБЕСПЕЧИВАЮЩИЙ АУТЕНТИФИКАЦИЮ КОНТЕЙНЕРА

А.А. Кобозева, М.А. Козина

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: alla_kobozeva@ukr.net

В работе получил дальнейшее развитие стеганографический метод двухэтапного декодирования дополнительной информации, основанный на решении систем линейных алгебраических уравнений, результатом которого стал стеганоалгоритм САБ-SIGN, обеспечивающий одновременное решение двух основных задач стеганографии – скрытой передачи данных и аутентификации контейнера, в качестве которого используется цифровое изображение, с соблюдением надежности восприятия стеганосообщения. Разработанный стеганоалгоритм является устойчивым к возмущающим воздействиям за счет обеспечения малого числа обусловленности задачи декодирования дополнительной информации, является эффективным при выявлении нарушения целостности стеганосообщения. Алгоритм САБ-SIGN является полиномиальным степени два.

Ключевые слова: стеганографический алгоритм, аутентификация, цифровое изображение, число обусловленности, матрица, система линейных уравнений

Введение

Одним из самых важных вопросов, решаемых обществом, на сегодняшний день является обеспечение защиты информации. В настоящий момент общество вступает в 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.

Актуальность проблемы информационной безопасности стимулирует создание новых алгоритмов и методов, позволяющих осуществлять ее защиту. Одно из перспективных направлений защиты информации сформировали современные методы стеганографии [2, 3]. Стеганография представляет собой совокупность методов, основывающихся на различных принципах, которые обеспечивают сокрытие самого факта существования конфиденциальной информации в той или иной среде, а также средств реализации этих методов. А именно, организация скрытого канала связи осуществляется внутри открытого канала: в некоторый контейнер, или основное сообщение (ОС), осуществляется внедрение дополнительной информации (ДИ) так, чтобы результат такого внедрения – стеганосообщение (СС) был зрительно неотличим от ОС [4].

Наибольшая активность на сегодня в научной деятельности в области стеганографии связана с ограничением использования шифрования во многих странах мира, в том числе и в Украине.

Особенность стеганографического подхода позволяет в рамках традиционно существующих информационных потоков или информационной среды решать некоторые важные задачи защиты информации ряда прикладных областей [3,4].

Одним из эффективных решений проблемы защиты авторского права, позволяющих проверить правообладателя цифровых изображений (ЦИ), видео-, звукозаписей, является организация обеспечения аутентичности за счет внедрения цифровых водяных знаков (ЦВЗ) [3]. Разработка методов встраивание ЦВЗ и встраивания ДИ с целью ее скрытой передачи образуют два основных направления развития современной стеганографии, решающих разные задачи. Исходя из важности и актуальности решения этих задач – аутентификации и организации скрытой передачи информации, в открытой печати предлагаются стеганоалгоритмы, осуществляющие их одновременное решение, однако имеющиеся разработки не лишены ряда существенных недостатков [5, 6], оставляя актуальной задачу разработки новых стеганографических алгоритмов, позволяющих одновременно обеспечивать скрытую передачу данных и аутентификацию сигнала-контейнера.

Цель исследования и постановка задания

Эффективность любого стеганографического метода (СМ) определяется рядом характеризующих его работу параметров, среди которых: гарантируемость обеспечения надежности восприятия стеганосообщения; устойчивость СМ к помехам – атакам; величина скрытой пропускной способности [3].

Известно, что на сегодняшний день при организации канала связи очень широко используется метод модификации наименьшего значащего бита (LSB). Однако при его весомых достоинствах, таких как, например, простой реализации, значительной скрытой пропускной способности, он имеет существенный недостаток, немаловажный при передаче СС в канале связи, связанный с чувствительностью СС к любого рода возмущающим воздействиям. В связи с этим в [7] был предложен СМ организации скрытой передачи данных, осуществляющий двухэтапное декодирование ДИ, основанный на решении систем линейных алгебраических уравнений (СЛАУ), позволивший значительно увеличить устойчивость к возмущающим воздействиям существующих стеганоалгоритмов, в частности, LSB, что было обосновано теоретически и проверено при помощи представительных вычислительных экспериментов. Однако разработанный в [7] метод, являясь привлекательным с точки зрения его устойчивости к атакам, не обеспечивает аутентификацию сигнала-контейнера. В связи с этим

Целью работы является модификация СМ двухэтапного декодирования ДИ [7] для обеспечения одновременного решения с его помощью двух основных задач стеганографии – скрытой передачи данных и аутентификации ОС с соблюдением надежности восприятия СС.

Для достижения цели в работе решаются следующие *задачи*:

1) несложной в вычислительном смысле организации пересылки и декодирования ДИ;

2) обеспечения малого числа обусловленности задачи декодирования ДИ;

3) организации обеспечения аутентификации ОС;

4) обеспечения эффективного декодирования ДИ в случае нарушения аутентичности для контейнера, в качестве которого выступает произвольное цифровое изображение.

Основная часть

В качестве ОС рассматривается цветное (модель RGB) ЦИ. СП будет проводится путем возмущения одной из трех матриц, отвечающих контейнеру, например, матрицы красной составляющей (хотя это не принципиально). Обозначим преобразуемую $n \times m$-матрицу контейнера F.

Стеганографическое преобразование изображения будет иметь характер матричных операций [8, 9], и в дальнейшем трактуется как возмущение ОС. Стеганосообщение при пересылке может подвергаться как преднамеренным, так и непреднамеренным атакам, что формализуется в виде дополнительных возмущающих воздействий и может привести к снижению эффективности декодирования ДИ.

Метод пересылки и декодирования ДИ, применяемый в области компьютерной стеганографии, будем называть устойчивым, если формируемое при помощи этого СМ стеганосообщение является нечувствительным (малочувствительным) к возмущающим воздействиям, т.е. декодирование полученной информации производится адресатом с малой результирующей ошибкой при наличии возмущающих воздействий в канале связи.

Разобьем матрицу контейнера F на $s \times s$-блоки (в частности, стандартным разбиением матрицы является разбиение на блоки размера 8×8 [10]). Пусть B — матрица произвольного блока. Далее все преобразования производятся с каждым блоком в отдельности.

В качестве ДИ будем рассматривать сформированный случайным образом бинарный вектор x длины $\left[\frac{n}{s}\right] \times \left[\frac{m}{s}\right]$, где $[\bullet]$ — целая часть аргумента, элементы которого $x_i \in \{-1,1\}$. ДИ может содержать и меньшее количество элементов, тогда она дополняется незначащими элементами до нужной длины.

В каждый блок B встраивается 1 бит ДИ — x_i после его предварительного кодирования, которое осуществляется следующим образом. Биту ДИ x_i ставится в соответствие вектор x^B с элементами $x^B{}_j$ длины s по следующему правилу:

$$x^B{}_j = \begin{cases} 1, \ если \ x_i = 1, \\ -1, \ если \ x_i = -1 \end{cases}, \quad j = \overline{1,s}.$$

Вектор x^B призван обеспечить в дальнейшем проверку аутентичности контейнера, а именно, его части, отвечающей блоку B.

Матрице блока B ставится в соответствие нижняя треугольная матрица $\overline{B}$ с элементами $\bar{b}_{ij}$, $i, j = \overline{1,s}$, в соответствии с соотношением:

$$\bar{b}_{ij} = \begin{cases} 1, если \ i = j, \\ 0, если \ i < j, \\ 1, если \ (i > j) \& (b_{ij} > t) \\ 0, если \ (i > j) \& (b_{ij} \le t) \end{cases}, \quad i, j = \overline{1,s}. \qquad (1)$$

Здесь $t = \dfrac{\max\limits_{i,j} f_{ij} + \min\limits_{i,j} f_{ij}}{2}$, где f_{ij} — элементы матрицы F. Матрица $\overline{B}$ по построению для любого блока B исходной матрицы F ОС нижняя треугольная, невырожденная ($\det \overline{B} = 1$), хорошо обусловленная.

Обозначим v — вектор длины s, отвечающий вектору x^B, получаемый следующим образом:

$$v = \overline{B} x^B. \qquad (2)$$

Вектор v, как следует из (2), будет иметь целые компоненты одного знака. Заметим, что при предположении отсутствия ошибок машинной арифметики, вектор x^B является точным решение системы линейных алгебраических уравнений

$$\overline{B}\, x^B = v. \tag{3}$$

Вектор v погружается в блок B, реализуя тем самым погружение информационного бита x_i ДИ. Для его элементов v_i, $i = \overline{1,s}$, из (2) с учетом вида $\overline{B}$ вытекает:

$$|v_i| \le s, \quad i = \overline{1,s}. \tag{4}$$

В отличии от [11], где аналогичный математический объект подвергается дополнительным преобразованиям для обеспечения надежности восприятия получаемого СС, соотношение (4) позволяет оставить сформированный в соответствии с (2) вектор v без преобразований: мы уходим от выбора дополнительного параметра m, от которого в [11] зависела эффективность декодирования ДИ.

В процессе СП для передачи по каналу связи одного бита x_i ДИ в матрицу B погружается вектор v: в каждый элемент *i*-ой строки блока аддитивно встраивается соответствующее значение v_i, $i = \overline{1,s}$.

При пересылке СС может подвергаться возмущающим воздействиям в канале связи, активным атакующим действиям, что естественным образом изменит его матрицу.

Декодирование ДИ адресатом включает в себя два этапа аналогично [11]. Матрица полученного СС разбивается на $s \times s$-блоки, обозначаемые далее B^S. Из каждого блока B^S на первом этапе декодирования ДИ извлекается в общем случае возмущенный вектор v, обозначаемый v^S, рассматриваемый как правая часть СЛАУ (3), где матрица СЛАУ отвечает нижней треугольной бинарной матрице, построенной для блока B^S аналогично (1), обозначаемая далее $\overline{B}^S$. Выделение информационного вектора $x^B{}_{np}$ с элементами $\left(x^B{}_{np}\right)_i$, $i = \overline{1,s}$, – приближенного для x^B происходит на втором этапе декодирования при решении неоднородной СЛАУ – в общем случае возмущенной системы (3), которая имеет вид:

$$\overline{B}^S x^B{}_{np} = v^S. \tag{5}$$

На этом этапе осуществляется проверка аутентичности ЦИ: в отсутствии возмущающих воздействий на СС при решении СЛАУ (5) для каждого блока матрицы СС

$$\left(x^B{}_{np}\right)_i = 1, \ i = \overline{1,s}, \quad \text{или} \quad \left(x^B{}_{np}\right)_i = -1, \ i = \overline{1,s},$$

что говорит о ненарушенной целостности контейнера. В противном случае СС было подвергнуто возмущающим воздействиям, претерпело несанкционированные изменения.

При выявлении нарушения целостности задача декодирования остается актуальной во многих случаях, в частности, если эти нарушения были непреднамеренными.

Для большинства изображений при малых возмущениях в канале связи $\overline{B}^S \approx \overline{B}$. Отличия этих матриц может быть в тех элементах, которые являются результатом кодирования элементов исходной матрицы из окрестности *t*. Таким образом, с

незначительным допущением в предположении малых возмущений можно считать, что система (5) отличается от системы (3) лишь вектором правой части. В этом случае $x^{B}{}_{пр} \neq x^{B}$. Учитывая вид множества, которому принадлежат элементы x^{B}, заметим, что для осуществления декодирования нас не столько интересуют непосредственные значения элементов $x^{B}{}_{пр}$, сколько их знак. Окончательный шаг декодирования отвечает формуле:

$$\left(\overline{x^{B}}_{пр}\right)_i = sign\left(\left(x^{B}{}_{пр}\right)_i\right), \quad i = \overline{1,s}. \tag{6}$$

Нужно отметить, что при нарушении целостности контейнера элементы вектора $\overline{x^{B}}_{пр}$ могут не оказаться равными. В этом случае предлагается бит ДИ x_i положить равным элементу $\overline{x^{B}}_{пр}$ с наибольшим повторением. Например: если вектор $\overline{x^{B}}_{пр}$ ($s = 8$), полученный в результате операции (6), содержит элементы (-1, -1, 1, 1, -1, -1, -1, -1), то $x_i = -1$.

В случае, когда число включений -1 и 1 в $\overline{x^{B}}_{пр}$ совпадает, то целесообразно брать во внимание знак, соответствующий последнему элементу вектора $\overline{x^{B}}_{пр}$: при получении именно последнего элемента вектора при кодировании, вероятнее всего получить наибольшее возмущение, которое далее не перекроется шумом атакующего, чтобы не привести к видимым нарушениям контейнера.

Вектор $\overline{x^{B}}$ будем называть sign-решением системы (3), а непосредственную реализацию алгоритма, идея которого предложена выше, будем называть САБ-SIGN.

Использование формулы (6) при декодировании, допускает неограниченно большие погрешности при решении (5), которые могут вообще не повлиять на результат декодирования (6), т.е. $\left\|\overline{x^{B}}_{пр} - x^{B}\right\|$ может быть сколь угодно велика, если при этом выполняются условия: $sign\left(x^{B}{}_i\right) = sign\left(\left(\overline{x^{B}}_{пр}\right)_i\right)$, $i = \overline{1,s}$. Таким образом, даже очень большие возмущения правой части системы при формировании v, о которых говорилось выше, сохраняющие знаки элементов вектора, могут не отразиться на результате декодирования.

Предложенный подход к решению СЛАУ дает возможность при декодировании получить ответ о нарушении/сохранении целостности контейнера, а также, как показывают результаты вычислительного эксперимента, получить большой объем правильно восстановленной информации даже при больших возмущениях входных данных.

Результаты вычислительного эксперимента.

Целью вычислительного эксперимента является практическая проверка эффективности разработанного стеганографического метода.

Одним из показателей, используемых для оценки эффективности метода является объем правильно восстановленной ДИ при одинаковых условиях проведения эксперимента, который вычисляется по формуле:

$$P = \frac{\text{Кол – во бит секретного сообщения, восстановленных верно}}{\text{Общее кол – во бит секретного сообщения}} \times 100\% \tag{1}$$

Все вычислительные эксперименты проводились в среде *MathWorks* MATLAB на 200 изображениях, сохраненных после СП, проводимого САБ-SIGN, в формате без

потерь. Возмущающие воздействия на СС моделировались путем наложения в пространственной области различных шумов с различными параметрами (табл. 1). Нарушение целостности СС в проведенном эксперименте было зафиксировано в 100% случаев, что говорит об эффективности использования САБ-SIGN с целью аутентификации ОС.

Таблица 1.

Зависимость объема правильно декодированной информации P от уровня шума, наложенного на стеганосообщение

Шум	Среднеквадратичное отклонение σ	P (%), при наложении шума	
		на все изображение	на красную составляющую изображения
Гауссовский	0.01	68	62
	0.001	82	71
	0.0001	96	94
	0.00001	99.9	98
Мультипликативный	0.01	87	87
	0.001	95	96
	0.0001	98	98
	0.00001	99.9	99
Пуассоновский		90	89

Процесс СП методом САБ-SIGN не нарушает надежность восприятия полученного СС, в отличие от процесса наложения аддитивного гауссовского шума со среднеквадратичным отклонением более 0.0001 (рис. 1), который, однако, сохраняет высокую эффективность декодирования ДИ (табл. 1). Результаты определялись как среднее арифметическое для 200 тестируемых ЦИ для каждого параметра шума.

Рассмотрим подробно вопрос выбора размера блока B. Из (4) следует, что наибольшие по модулю значения элементов вектора v, равны s. Уменьшение/увеличение размера блока приведет к уменьшению/увеличению возмущения пикселей ЦИ-контейнера в процессе СП. Чем больше размер блока, на который разбивается матрица ОС, тем больше эта матрица получит возмущение в процессе погружения ДИ, что, во-первых, приведет к уменьшению чувствительности СС к возмущающим воздействиям, что является положительным фактором (см. рис. 3, 4), но, во-вторых, может привести к нарушению надежности восприятия СС, а в-третьих, уменьшит скрытую пропускную способность организуемого стеганографического канала связи.

Заметим, что не целесообразно использовать блоки, для которых $s < 4$. Действительно, в этом случае, с учетом (4), СП приведет к незначительным возмущениям матрицы ОС, результатом чего станет СС, чувствительное к любым возмущающим воздействиям.

Как следует из результатов вычислительного эксперимента (рис. 3, 4), наиболее предпочтительным с точки зрения устойчивости является САБ-SIGN, использующий блоки размера 16×16. Однако использование таких блоков может привести к нарушению надежности восприятия СС, а также уменьшает в четыре (шестнадцать) раза скрытую пропускную способность организуемого канала связи, по сравнению с 8×8- (4×4-) блоками. В тоже время объем P верно декодированной информации в случае 16×16-блоков незначительно отличается от значения P при выборе блока размером 8×8. Таким образом, для САБ-SIGN рекомендуется использовать блоки стандартного разбиения - 8×8.

а

б

в

г

д

Рис. 1. Изображение Image и его преобразования путем внедрения ДИ и наложения аддитивного гауссовского шума с нулевым матожидаем и различными значениями среднеквадратичного отклонения σ: а – исходное ЦИ; б – СС; в – $\sigma = 0.01$; г – $\sigma = 0.001$; д – $\sigma = 0.0001$

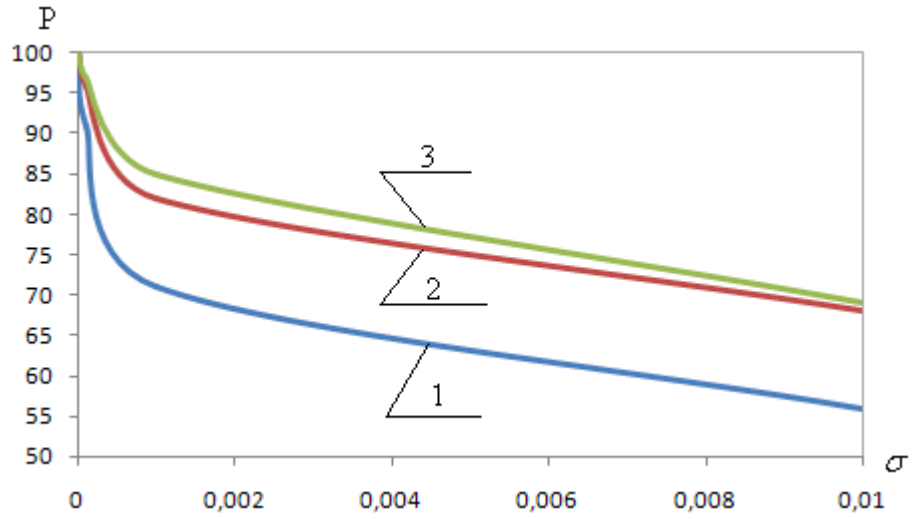

Рис. 3. Зависимость объема декодированной информации от параметра накладываемого на СС аддитивного гауссовского шума при различных размерах блока матрицы: 1 – $s=4$; 2 – $s=8$; 3 – $s=16$

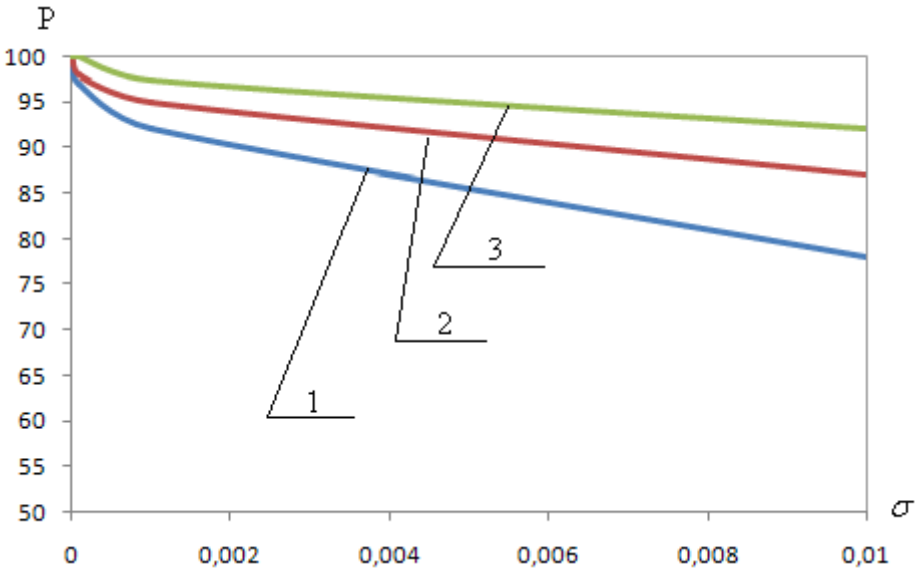

Рис. 4. Зависимость объема декодированной информации от параметра накладываемого на СС мультипликативного шума при различных размерах блока матрицы: 1 – $s=4$; 2 – $s=8$; 3 – $s=16$

Заключение

В работе предложена модификация СМ двухэтапного декодирования ДИ, основанного на решении СЛАУ, обеспечивающая одновременное решение двух основных задач стеганографии – скрытой передачи данных и аутентификации контейнера с соблюдением надежности восприятия СС.

Разработанный стеганоалгоритм САБ-SIGN является устойчивым к возмущающим воздействиям за счет обеспечения малого числа обусловленности задачи декодирования ДИ. Объем восстановленной ДИ в условиях наложения шума составил $P > 90\%$ при $\sigma < 0.001$ для аддитивного гауссовского и мультипликативного шумов, что говорит о высокой эффективности САБ-SIGN.

При нарушении целостности СС, сформированного САБ-SIGN, это нарушение было выявлено в 100% случаев.

Вычислительная сложность разработанного алгоритма определяется как $\underline{O}\left(n^2\right)$ для $n \times n$-матрицы контейнера.

Все вышесказанное позволяет утверждать, что цель работы достигнута.

Список литературы

1. Хорошко, В.А. Методы и средства защиты информации [Текст] : научное издание / В.А. Хорошко, А.А. Чекатков; Ред. Ю.С. Ковтанюк. — К. : ЮНИОР, 2003. — 505 с.
2. Кобозєва, А.А. Аналіз захищеності інформаційних систем / А.А. Кобозєва, І.О. Мачалін, В.О. Хорошко. — К. : Вид. ДУІКТ, 2010. — 316 с.
3. Грибунин, В.Г. Цифровая стеганография [Текст] : монография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. — М. : СОЛОН-Пресс, 2002. — 272 с.
4. Конахович, Г.Ф. Компьютерная стеганография [Текст]: теория и практика / Г.Ф. Конахович, А.Ю. Пузыренко. — Киев : МК-Пресс, 2006. — 288 с.
5. 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. — Том 35, № 2. — С. 262–267.
6. Кобозева, А.А. Стеганографический алгоритм скрытой передачи информации, обеспечивающий аутентификацию контейнера / А.А. Кобозева, А.Д. Шовкун // Науковий вісник Міжнародного гуманітарного університету. Серія: Інформаційні технології та управління проектами. — 2012. — № 4. — С. 21–28.
7. Кобозева, А.А. Стеганографический метод, основанный на решении систем линейных алгебраических уравнений / А.А. Кобозева, А.В. Коломийчук // Праці УНДІРТ. — 2006. — № 1(45)–2(46). — С. 104–108.
8. Деммель, Д. Вычислительная линейная алгебра [Текст] : теория и приложения / Д. Деммель; Пер. с англ. Х.Д. Икрамова. — М. : Мир, 2001. — 430 с.
9. Гантмахер, Ф.Р. Теория матриц [Текст] : монография / Ф.Р. Гантмахер. — 5-е изд. — М. : Физматлит, 2004. — 559 с.
10. Гонсалес, Р. Цифровая обработка изображений / Р. Гонсалес, Р. Вудс; пер. с англ. П.А. Чочиа. — М. : Техносфера, 2006. — 1070 с.
11. Кобозева, А.А. Практическая реализация стеганографического метода, основанного на решении системы линейных алгебраических уравнений / А.А. Кобозева, И.И. Борисенко // Праці УНДІРТ. — 2006. — № 3(47). — С. 78–83.

СТЕГАНОГРАФІЧНИЙ МЕТОД ДВОЕТАПНОГО ДЕКОДУВАННЯ, ЩО ЗАБЕЗПЕЧУЄ АУТЕНТИФІКАЦІЮ КОНТЕЙНЕРА

А.А. Кобозєва, М.О. Козіна

Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: alla_kobozeva@ukr.net

У роботі отримав подальший розвиток стеганографічний метод двоетапного декодування додаткової інформації, заснований на рішенні систем лінійних алгебраїчних рівнянь, результатом якого став стеганоалгоритм САБ-SIGN, що забезпечує одночасне рішення двох основних задач стеганографії – прихованої передачі даних і автентифікації контейнера, у якості якого використовується цифрове зображення, з дотриманням надійності сприйняття стеганоповідомлення. Розроблений стеганоалгоритм є стійким до збурних дій за рахунок забезпечення малого числа обумовленості задачі декодування додаткової інформації, є ефективним при виявленні порушення цілісності стеганоповідомлення. Алгоритм САБ-SIGN є поліноміальним ступеня два.

Ключові слова: стеганографічний алгоритм, автентифікація, цифрове зображення, число обумовленості, матриця, система лінійних рівнянь

THE STEGANOGRAPHIC METHOD WITH A TWO-STAGE DECODING WHICH PROVIDS AUTHENTIFICATION THE CONTAINER

Alla A. Kobozeva, Mariya A. Kozina

Odessa National Polytechnic University,
1 Shevchenko Ave., Odessa, 65044, Ukraine; e-mail: alla_kobozeva@ukr.net

The steganographic method with a two-stage decoding of additional information, based on the decision of the systems of linear algebraic equalizations, the result of which has become steganoalgorithm SAB-SIGN, providing at the same time the decision for two basic tasks of steganography – the hidden data of communication and authentification the container as digital image, with the observance of reliability perception of steganomessage, has got further development in this article. Steganoalgorithm which was developed is steady to revolting influences due to providing a small number of conditionality of the task with decoding the additional information, is effective at the exposure of violation integrity of the steganomessage. An algorithm of SAB-SIGN is polynomial with second degree.

Keywords: steganographic algorithm, authentication, digital image, number of conditionality, matrix, system of linear equalizations