УДК 004.056.5

А.А. Кобозева,
Л.М. Дзюбинская,
И.И. Бобок

СТЕГАНОПРЕОБРАЗОВАНИЕ ПРОСТРАНСТВЕННОЙ ОБЛАСТИ ЦИФРОВОГО ИЗОБРАЖЕНИЯ, УСТОЙЧИВОЕ К МАСШТАБИРОВАНИЮ

В работе предложено усовершенствование устойчивого к атакам против встроенного сообщения, не меняющим геометрию изображения, стеганоалгоритма, разработанного на основе достаточного условия устойчивости, полученного ранее одним из авторов в пространственной области изображения-контейнера, с целью обеспечения эффективной работы алгоритма в условиях комплексной атаки, составной частью которой является геометрическая атака масштабированием изображения-стеганосообщения. Приведены результаты вычислительного эксперимента, подтверждающие высокую эффективность предложенной модификации стеганоалгоритма в упомянутых условиях.

***Ключевые слова**: стеганографический алгоритм, устойчивость к атакам против встроенного сообщения, геометрические атаки, масштабирование, пространственная область изображения.*

У роботі запропоновано вдосконалення стійкого до атак проти вбудованого повідомлення, які не змінюють геометрію зображення, стеганоалгоритму, розробленого на основі достатньої умови стійкості, отриманої раніше одним з авторів в просторовій області зображення-контейнера, з метою забезпечення ефективної роботи алгоритма в умовах комплексної атаки, складовою частиною якої є геометрична атака масштабуванням зображення-стеганоповідомлення. Наведені результати обчислювального експерименту, які підтверджують високу ефективність запропонованої модифікації стеганоалгоритму в наведених умовах.

***Ключові слова**: стеганографічний алгоритм, стійкість до атак протии вбудованого повідомлення, геометричні атаки, масштабування, просторова область зображення.*

The improvement of the image, resistant to the attacks against embedded messages, without changing the geometry as well as a steganogram, developed on the basis of sufficient stability conditions obtained previously by one of the authors in the spatial domain of the image-container, with the aim of the ensuring the effective operation of the algorithm in terms of complex attacks, the part of which is the geometric attack of the image steganomessage, is suggested. The results of the computational experiment, confirming the high efficiency of the proposed modification steganogram in the above-mentioned conditions are stated.

***Keywords:** steganographic algorithm, resistance to attacks against embedded messages, geometric attacks, scaling, spatial area of the image.*

Введение

Стеганографические методы являются важной обязательной составляющей любой современной комплексной системы защиты информации [1, 2].

К стеганографическому методу, алгоритму, используемому для организации скрытого канала связи, предъявляется ряд требований [2–4]:

устойчивость к атакам против встроенного сообщения;

устойчивость к стеганоанализу;

обеспечение надежности восприятия стеганосообщения, являющегося результатом стеганопреобразования контейнера;

обеспечение достаточной скрытой пропускной способности [2];

незначительная вычислительная сложность.

Таким образом, устойчивость к атакам против встроенного сообщения, целью которых является полное/частичное разрушение встроенной в контейнер дополнительной информации (ДИ) за счет возмущения стеганосообщения, является одним из основных требований к стеганографическому алгоритму (СА), задача обеспечения которого до настоящего момента не решена полностью [2, 3, 5].

В качестве контейнера в настоящей работе с учетом частоты использования в современных условиях выбрано цифровое изображение (ЦИ).

Среди атак против встроенного сообщения наиболее распространенными являются:

атаки, не меняющие геометрию изображения: фильтрация стеганосообщения, наложение шума, сжатие стеганосообщения с потерями;

– геометрические атаки: обрезка ЦИ-стеганосообщения, масштабирование, поворот ЦИ или его части, параллельный перенос некоторой части ЦИ в пределах этого изображения.

Наиболее пагубными атаками по результату воздействия на стеганосообщение являются последние, при этом возможности противодействия таким атакам и эффективность имеющихся способов оставляют желать лучшего [2, 3].

Подавляющее большинство существующих устойчивых стеганоалгоримов осуществляют погружение ДИ в области преобразования контейнера (частотной области, области сингулярного, спектрального разложения матрицы изображения и т.д.), не учитывая при этом преимущества, которые дает организация стеганопреобразования и декодирования ДИ в пространственной области ЦИ-контейнера. Однако в [6] была обоснована принципиальная возможность обеспечения более высокой устойчивости для стеганоалгоритмов, которые работают в пространственной области ЦИ, по сравнению со СА, работающими в областях преобразования. В [6] было доказано, что для обеспечения устойчивости СА к атаке против встроенного сообщения, результат действия которой на $l \times l$ – блок $\overline{B}$ матрицы стеганосообщения оценивается как $\left\| \Delta \overline{B} \right\|_2$, достаточно, чтобы стеганопреобразование, которое проводится в пространственной области ЦИ-контейнера, формально представлялось в виде возмущений яркости всех пикселей каждого блока, задействованного в стеганопреобразовании, на величину Δb, для которой имеет место соотношение:

$$|\Delta b| > \left\| \Delta B \right\|_2 / l. \qquad (1)$$

Упомянутое достаточное условие обеспечило устойчивость разработанного на его основе в [7] стеганоалгоритма. Однако устойчивость к геометрическим атакам в [7] не рассматривалась, а задача обеспечения такой устойчивости вообще не ставилась.

Цель статьи и постановка заданий

Одной из самых распространенных и легко реализуемых геометрических атак, направленных против встроенного сообщения, является масштабирование стеганосообщения. Масштабирование ЦИ реализовано в любом графическом редакторе (например, Photoshop), программных средах (например, Matlab).

Целью работы является усовершенствование разработанного в [7] на основе достаточного условия устойчивости СА к атакам против встроенного сообщения, полученного в [6], базового стеганоалгоритма SA_B, обеспечивающее его устойчивость в условиях комплексной атаки, обязательной составной частью которой является геометрическая атака масштабированием.

Для достижения цели необходимо решить следующие *задачи*:

1. Проанализировать устойчивость разработанного в [7] стеганоалгоритма SA_B к атаке масштабированием;

2. Усовершенствовать стеганоалгоритм SA_B таким образом, чтобы он оказался устойчивым к атаке масштабированием;

3. Провести вычислительный эксперимент с целью оценки устойчивости усовершенствованного алгоритма в условиях комплексной атаки против встроенного сообщения, обязательной составной частью которой является геометрическая атака масштабированием.

Основная часть

Формальным представлением ЦИ-контейнера в работе служит двумерная $n \times m$ матрица F. Заметим, что это никак не ограничивает общность рассуждений и область применимости предлагаемого ниже стеганометода, поскольку в случае цветного ЦИ погружение ДИ происходит часто лишь в одну матрицу − цветовую составляющую. Если же стеганопреобразование будет проходить для нескольких/всех матриц ЦИ-контейнера, то предпринимаемые при погружении ДИ действия, описанные ниже, могут быть проделаны с каждой цветовой составляющей в отдельности.

В качестве ДИ рассматривается сформированная случайным образом бинарная последовательность $p_1, p_2, ..., p_t$, $p_i \in \{0,1\}$ для $i = \overline{1,t}$.

Устойчивость стеганоалгоритма к возмущающим воздействиям оценивается стандартным образом: значением коэффициента корреляции (NC) для ДИ, который определяется в соответствии с формулой [7]:

$$NC = \frac{\sum_{i=1}^{t} p_i' \times \overline{p}_i'}{t},$$

где $\overline{p}_1, \overline{p}_2, ..., \overline{p}_t$ − декодированная ДИ, $\overline{p}_i \in \{0,1\}$, $i = \overline{1,t}$; $p_i' = 1$, $\overline{p}_i' = 1$, если $p_i = 1$, $\overline{p}_i = 1$; $p_i' = -1$, $\overline{p}_i' = -1$, если $p_i = 0$, $\overline{p}_i = 0$. Таким образом, значения $p_i' \times \overline{p}_i' \in \{1,-1\}$.

Ключевым моментом для разработанного в [7] на основе достаточного условия устойчивости СА к атакам против встроенного сообщения базового стеганоалгоритма SA_B, работающего в пространственной области ЦИ-контейнера, является неизменность геометрии изображения: погружение и декодирование ДИ осуществляется при строгом геометрическом соответствии блоков матриц контейнера и стеганосообщения – совпадение размеров, месторасположения в пределах матрицы изображения. В силу этого использование базового СА SA_B в условиях атаки масштабированием, меняющей размеры ЦИ, а значит, и размеры соответствующих блоков в матрице стеганосообщения относительно блоков матрицы контейнера, принципиально не может быть эффективным, что подтверждается результатами вычислительного эксперимента, в котором было задействовано 500 ЦИ в разных форматах хранения (с потерями, без потерь), проведенного в среде Matlab.

Для адаптации к условиям масштабирования необходимо обеспечить возможность совпадения размеров соответствующих блоков матриц контейнера (использованных при стеганопреобразовании) и возмущенного стеганосообщения перед осуществлением декодирования ДИ.

Реализация обозначенного требования при наличии контейнера для декодирования ДИ является принципиально возможной. Необходимо отметить, что в большинстве современных научных публикаций по обсуждаемой теме требование наличия контейнера для декодирования пересылаемой информации рассматривается как недостаток СА, с чем не согласны авторы настоящей работы: для "неслепого" стеганографического алгоритма контейнер является частью секретного ключа, значительно понижая вероятность декодирования пересылаемой дополнительной информации атакующей стороной при перехвате стеганосообщения.

Таким образом, предлагаемая ниже модификация СА SA_B оставляет алгоритм "неслепым". Погружение ДИ осуществляется в соответствии с [7], а вот в декодирование вносятся изменения, имеющие целью обеспечить совпадения размеров соответствующих блоков матриц контейнера и стеганосообщения, задействованных при погружении/декодировании пересылаемой информации. Результатом модификации SA_B, предложенной ниже, является стеганографический метод, далее обозначаемый как SA_m.

Основные шаги SA_m следующие.

Погружение ДИ.

1. Матрица F ЦИ-контейнера розбивается стандартным образом [8] на непересекающиеся $l \times l$ блоки.

2. Пусть B – очередной $l \times l$ блок контейнера, который используется для стеганопреобразования, а p_i – очередной бит ДИ, $\overline{B}$ – соответствующий блок стеганосообщения.

Если

$$p_i = 1$$

то

$$\overline{B} = B + \Delta b \cdot \overline{E}$$

иначе

$$\overline{B} = B - \Delta b \cdot \overline{E}$$

где $\overline{E}$ – $l \times l$– матрица, все элементы которой равны 1, $\Delta b > 0$ удовлетворяет (1).

Декодирование ДИ

1. Пусть F, $\overline{\overline{F}}$ – $n \times m$ и $\overline{\overline{n}} \times \overline{\overline{m}}$ матрицы контейнера и возмущенного стеганосообщения соответственно.

Если

$$\begin{bmatrix} n \neq \overline{\overline{n}}, \\ m \neq \overline{\overline{m}}, \end{bmatrix}$$

то

вычислить $\frac{\overline{\overline{n}}}{n}, \frac{\overline{\overline{m}}}{m}$.

Если

$$\frac{\overline{\overline{n}}}{n} = \frac{\overline{\overline{m}}}{m},$$

то считается, что стеганосообщение претерпело атаку масштабированием с коэффициентом $\frac{\overline{\overline{n}}}{n} = \frac{\overline{\overline{m}}}{m}$.

2. Провести (обратное) масштабирование стеганосообщения с $\overline{\overline{n}} \times \overline{\overline{m}}$ – матрицей $\overline{\overline{F}}$ с коэффициентом $\frac{n}{\overline{\overline{n}}} = \frac{m}{\overline{\overline{m}}}$. Результат – $n \times m$ – матрица $\tilde{F}$.

3. Разбить стандартным образом матрицы F и $\tilde{F}$ на непересекающиеся $l \times l$– блоки, обозначаемые B и $\tilde{B}$ соответственно. Каждый блок $\tilde{B}$ используется для декодирования одного бита ДИ.

4. Пусть $\tilde{B}$ – очередной блок $\tilde{F}$, из которого декодируется бит $\overline{p}_i$ ДИ, а B – соответствующий блок контейнера.

2.1. Определить:

$$\Delta \tilde{B} = \tilde{B} - B.$$

2.2. Определить количества положительных k_p и отрицательных k_n элементов в матрице $\Delta \tilde{B}$.

если

$$k_p > k_n,$$

то

$$\overline{p}_i = 1,$$

иначе

$$\overline{p}_i = 0$$

Конкретный алгоритм, реализующий стеганометод SA_m, определяется значениями l, Δb, а также видом интерполяции, которая используется для организации обратного масштабирования на шаге 2 декодирования ДИ.

Для проверки устойчивости стеганоалгоритмов, реализующих SA_m в условиях атак против встроенного сообщения, был проведен вычислительный эксперимент, в котором:

– было задействовано 500 цветных ЦИ размером пикселей (цветовая схема RGB), хранимых в различных форматах (с потерями (Jpeg), без потерь (Tif)), полученных из базы NRCS [9] (которая является традиционной при тестировании алгоритмов, работающих с ЦИ), а также изображения, полученные непрофессиональными фотографами;

– $l = 8$, $\Delta b = 9$ [7].

В ходе эксперимента погружение ДИ проводилось в синюю цветовую составляющую ЦИ-контейнера, после чего ЦИ-стеганосообщение сохранялось в формате с потерями (Jpeg). Очевидно, что такое сохранение уже само по себя является атакой против встроенного сообщения, однако его проведение оправдано и целесообразно в силу следующих причин. В настоящее время хранение и передача цифровых сигналов по каналам телекоммуникаций в связи со значительным увеличением объемов информации осуществляется в сжатом состоянии. Этот факт не может не учитываться при организации стеганографического канала связи: в современном мультимедийном пространстве дополнительное внимание привлекает пересылка ЦИ, цифрового видео в форматах без потерь. В силу этого для дополнительной скрытности организуемого канала связи целесообразным является еще на этапе формирования стеганосообщения его сохранение в формате с потерями с использованием для стеганопреобразования необходимо устойчивых к сжатию стеганометодов и алгоритмов, какими и являются SA_B и SA_m.

В ходе эксперимента атака масштабированием на стеганосообщение проводилась в графическом редакторе *Adobe Photoshop*, а также в среде *Matlab* с использованием бикубической (*bicubick*), билинейной интерполяции (*bilinear*), ближайшего соседа (*nearest*). Поскольку результаты, характеризующие устойчивость реализаций метода SA_m в условиях атак (значения *NC*), включающих масштабирование, практически не отличались, далее приводятся результаты экспериментов, проведенных в среде *Matlab*.

Необходимо отметить, что при проведении обсуждаемой геометрической атаки с большой вероятностью коэффициент масштабирования k, используемый атакующим, будет незначительным: размеры возмущенного стеганосообщения не должны отличаться от размеров оригинального значительно, чтобы не привлечь внимание сторон, организующих стеганографический канал связи. Однако в целях повышения объективности результатов тестирования реализаций SA_m при проведении вычислительного эксперимента коэффициенты масштабирования выбирались не только малыми (см. табл. 1, 2).

После атаки масштабированием возмущенное стеганосообщение сохранялось в силу указанных выше причин в формате с потерями (Jpeg), обеспечивая тем самым очередную (вторую) атаку сжатием против встроенного сообщения, после чего происходило декодирование ДИ.

Таким образом, с учетом перечисленных выше факторов в реальных условиях атака против встроенного сообщения при наличии масштабирования будет носить комплексный характер, составляющие которой следующие:

1. Сжатие стеганосообщения с потерями (на этапе формирования);
2. Масштабирование стеганосообщения;
3. Сжатие возмущенного масштабированием стеганосообщения с потерями.

В табл. 1 приведены результаты декодирования ДИ алгоритмом, реализующим метод SA_m в условиях описанной комплексной атаки против встроенного сообщения в случае, когда способ интерполирования при атаке масштабированием совпадал со способом интерполирования при обратном масштабировании, выполняемом на шаге 2 декодирования ДИ. Эта часть эксперимента имела своей целью выбор наиболее предпочтительного с точки зрения обеспечения устойчивости SA_m способа интерполирования для проведения обратного масштабирования в SA_m, поскольку в реальных условиях вероятность совпадения способа интерполяции при атаке масштабированием и обратном масштабировании очевидно мала.

Таблица 1

Устойчивость реализации метода SA_m в условиях совпадения способов интерполирования, использованных при масштабировании при атаке на стеганосообщение и декодировании ДИ (среднее значение *NC* по 500 ЦИ)

Вид интерполяции \ k	1.01	0.99	1.5	0.5	2
bicubick	0.9752	0.9682	0.9845	0.8192	0.9889
bilinear	0.9684	0.9587	0.9843	0.7488	0.9792
nearest	0.9771	0.9660	0.9891	0.8341	0.9867

Как свидетельствуют результаты, приведенные в табл. 1, предпочтительным является использование для обратного масштабирования на шаге 2 декодирования ДИ при реализации метода SA_m видов интерполяции *bicubick* и *nearest*.

Результаты эксперимента, в случае, когда для обратного масштабирования в реализации SA_m использовался способ интерполяции *nearest*, приведены в табл. 2.

Таблица 2

Устойчивость SA_m в условиях несовпадения способов интерполирования, использованных при масштабировании при атаке на стеганосообщение, со способом *nearest*, использованным при декодировании ДИ (среднее значение *NC* по 500 ЦИ)

Вид интерполяции при атаке \ k	1.01	0.99	1.5	0.5	2
bicubick	0.9607	0.9607	0.9824	0.8252	0.9819
bilinear	0.9585	0.9586	0.9808	0.7916	0.9762

Как свидетельствуют полученные результаты (табл. 1, 2), стеганометод SA_m при его проведенных реализациях является устойчивым в условиях комплексной атаки против встроенного сообщения, включающей в себя геометрическую атаку масштабированием. Из общей положительной картины выбивается случай масштабирования с коэффициентом k=0.5, при котором среднее по всем 500 ЦИ значение $NC < 0.84$ для всех рассмотренных вариантов интерполирования. Такая ситуация является следствием следующего: при атаке на стеганосообщение с

его линейные размеры уменьшаются в 2 раза, вызывая при этом потерю оригинальной вложенной в контейнер ДИ. Обратное масштабирование хоть и "вернет" ЦИ к первоначальным размерам, используя средства интерполяции, но восстановить качественно и количественно утерянную ДИ принципиально не в состоянии. Априори ожидаемым является менее эффективное декодирование ДИ при реализации SA_m в условиях атаки масштабированием на стеганосообщение с коэффициентом $k<1$, по сравнению с результатами декодирования при $k>1$, что находится в полном соответствии с результатами, приведенными в табл. 1, 2. Для удобства дополнительного анализа этих результатов обозначим $\Delta = NC^{(2)} - NC^{(1)}$, где $NC^{(2)}$ и $NC^{(1)}$ – значения коэффициентов корреляции ДИ, полученных для одного вида и одного коэффициента интерполяции в условиях, используемых для получения данных табл. 1, 2 соответственно. На первый взгляд кажется, что несовпадение способов интерполирования при выполнении первичного (при атаке) и обратного масштабирования стеганосообщения должно привести к понижению устойчивости SA_m по сравнению с вариантом их совпадения, однако, как свидетельствуют результаты, приведенные на рис. 1, это не всегда так. Для приведенных данных исключение составляет вариант, отвечающий k=0.5, что говорит о необходимости дополнительных исследований процесса масштабирования с коэффициентом $k<1$, на что направлены усилия авторов в настоящий момент.

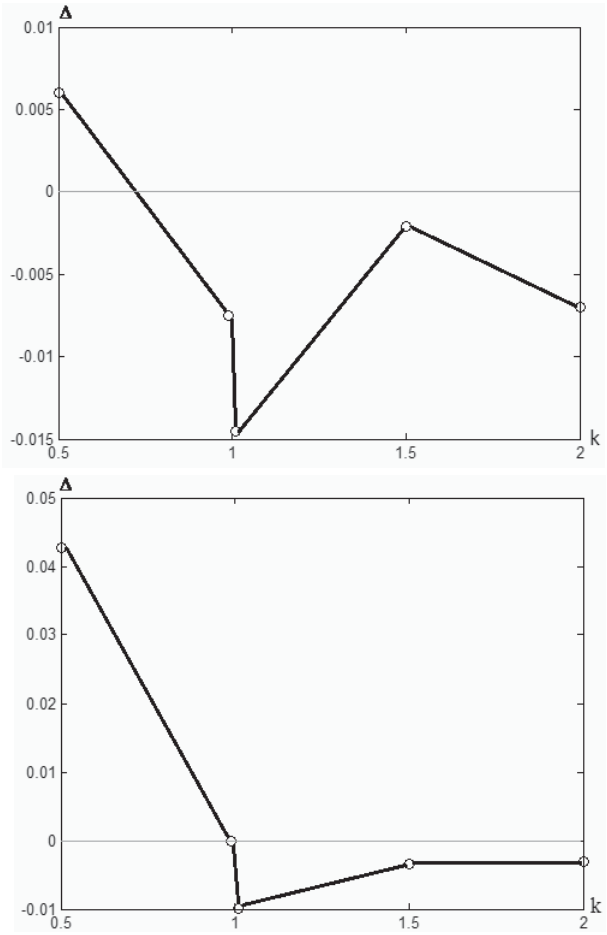

Рис. 1. Зависимость Δ – изменения устойчивости СА SA_m при несовпадении видов интерполирования при прямом и обратном масштабировании стеганосообщения, по сравнению с вариантом их совпадения, от коэффициента масштабирования k, в случае, когда при атаке используется: а – *bicubick* ; б – *bilinear* (интерполяция)

Заключение

В работе предложен стеганографический метод SA_m, работающий в пространственной области изображения, являющийся усовершенствованием устойчивого к атакам против встроенного сообщения, не меняющим геометрию изображения, стеганоалгоритма SA_B, предложенного ранее в [7]. Результатом усовершенствования явилась устойчивость реализаций метода в условиях комплексной атаки, состоящей из двукратного сжатия с потерями и масштабирования стеганосообщения, что подтверждается полученными результатами вычислительного эксперимента.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. *Ленков С.В.* Методы и средства защиты информации : в 2 т. / С.В. Ленков, Д.А. Перегудов, В.А. Хорошко. – К. : Арий, 2008. – Т. 2 : Информационная безопасность. – 2008. – 344 с.

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

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

4. *Конахович Г.Ф.* Компьютерная стеганография : теория и практика / Г.Ф. Конахович, А.Ю. Пузыренко. – Киев : МК-Пресс, 2006. – 288 с.

5. *Кобозєва А.А.* Аналіз захищеності інформаційних систем : підруч. для студ. вищ. навч. закл., які навч. за напр. "Інформаційна безпека" та "Системні науки та кібернетика" / А.А. Кобозєва, І.О. Мачалін, В.О. Хорошко ; Мін-во трансп. та зв'язку України, Держ. ун-т інформ.-комунікац. технологій. – К. : ДУІКТ, 2010. – 316 с.

6. *Кобозева А.А.* Условия обеспечения устойчивости стеганоалгоритма при организации стеганопреобразования в пространственной области контейнера-изображения / А.А. Кобозева, О.В. Костырка // Інформаційна безпека. – 2013. – № 3(11). – С. 29–35.

7. *Костирка О.В.* Стеганографічний алгоритм, стійкий до накладання шуму / О.В. Костирка // Безпека інформації. – 2014. – Т. 20, № 1. – С. 71–75.

8. *Гонсалес Р.* Цифровая обработка изображений / Р. Гонсалес, Р. Вудс ; пер. с англ. П.А. Чочиа. – М. : Техносфера, 2006. – 1070 с.

9. NRCS Photo Gallery // United States Department of Agriculture. Washington, USA [Електронний ресурс]. – Режим доступу : http : // photogallery.nrcs.usda.gov (Дата звернення : 26.07.2012).

Отримано 10.09.2014

Рецензент Рибальський О.В., доктор технічних наук, професор.