УДК 004

И.И. Борисенко

СЕГМЕНТАЦИЯ КОНТЕЙНЕРА В СТЕГАНОГРАФИЧЕСКИХ АЛГОРИТМАХ ПРОСТРАНСТВЕННОЙ ОБЛАСТИ ВСТРАИВАНИЯ

Работа посвящена решению задачи повышения устойчивости стеганографических алгоритмов пространственной области встраивания к возмущающим воздействиям. Используется сегментация блоков контейнера как один из эффективных инструментов предобработки матрицы контейнера.

Ключевые слова: *стеганография, контейнер, стеганографический контейнер, сегментация.*

Робота присвячена вирішенню завдання підвищення стійкості стеганографічних алгоритмів просторової області вбудовування до збурних дій. Використовується сегментація блоків контейнера як один з ефективних інструментів попередньої обробки матриці контейнера.

Ключові слова: *стеганографія, контейнер, стеганографічний контейнер, сегментація.*

This paper is devoted to the solving of the problem of the improving of the resist to the perturbation of the spatial domain steganographic algorithms. Segmentation of container blocks, as one of the efficiency instruments for pred-processing of the matrix of container, is used.

Keywords: *steganography, container, stego, segmentation.*

Введение

Общение в современном обществе немыслимо без использования компьютерных сетей, постоянное совершенствование которых обостряет вопрос безопасности информации, которая циркулирует в сетевой среде. Широкое применение как способ осуществления скрытой связи получили методы компьютерной стеганографии. Изображение, видео, аудио, которые используются для сокрытия секретной информации (СИ), принято называть контейнером, после встраивания информации контейнер становится стеганоконтейнером, который открыто передается сетевыми каналами получателю. Основное свойство, которому должен удовлетворять стеганографический метод, – это устойчивость к обнаружению скрытой СИ, которое, понятно, не гарантирует обеспечение эффективности ее декодирования при передаче стеганоконтейнера (СК) по сети. Поэтому на современном этапе все более значимой становится задача обеспечения устойчивости стеганометодов (СМ) и стеганоалгоритмов (СА) к активным возмущающим воздействиям, которым может подвергнуться СК при передаче, например, к шумам в канале связи.

Несмотря на то, что СМ, внедряющие СИ в область преобразования контейнера, считаются более устойчивыми, многие авторы [1–3 и др.] посвящают свои работы разработке СМ и СА пространственной области встраивания в силу ряда преимуществ, которые при этом достигаются, – такие алгоритмы не используют дополнительные вычислительные и временные ресурсы для перехода в область преобразования, а также объем внедряемой СИ в контейнер (так называемая скрытая пропускная способность) больше, чем у спектральных СА. Вопрос устойчивости к активным возмущениям таких алгоритмов остается актуальным.

Целью данной работы является повышение устойчивости стеганографических алгоритмов пространственной области встраивания к возмущающим воздействиям. Для достижения цели были поставлены и решены задачи: анализа СА с малой устойчивостью к возмущающим воздействиям и исследования возможности ее повышения на основе известных методов и подходов; разработки более устойчивых модификаций на основе существующих неустойчивых СА.

Обзор базовых алгоритмов

В работе [4] представлен алгоритм “Payload Transformation”, первым шагом которого является разбивка контейнера-изображения на блоки размером 2*2: $X = \begin{bmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{bmatrix}$. Блоки проверяются на уникальность строк, если строки совпадают, то яркость одного из элементов строки изменяется для выполнения условия уникальности. Далее выполняется проверка разностей яркости элементов блока вида: $x_{11} - x_{12}$, $x_{11} - x_{21}$, $x_{21} - x_{22}$. Полученные разности не должны превышать наперед заданную величину порогового значения Δ, что обеспечит надежность восприятия контейнера (искажения, вносимые при погружении СИ, визуально не будут заметны). Если одна из вычисленных разностей превышает пороговое значение, то блок не используется для внедрения СИ, таким образом, пороговое условие используется для выбора блоков, которые не попадают в область изображения, где присутствует резкое изменение интенсивности.

Секретная информация, которая встраивается, представляется в виде бинарной последовательности. В каждый блок встраивается два бита СИ.

Рассматривается единичная матрица $H = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, которая подвергается определенному виду преобразования в зависимости от вида встраиваемой бинарной пары СИ.

– Если встраивается пара (00), то матрица H остается без изменений.

– Если встраивается пара (01), то матрица H преобразуется к виду $H_T = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}$.

– Если встраивается пара (10), то матрица H преобразуется к виду $H_T = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}$.

– Если встраивается пара (11), то матрица H преобразуется к виду $H_T = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$.

Далее полученная матрица H_T умножается на матрицу блока, т.е. выполняется стеганопреобразование по правилу $Y= H_T*X$. В результате такого преобразования формируется стеганоконтейнер, блоки которого имеют отличительную особенность: если встраивалась пара бит (01) или (10), то строки блока получаются одинаковыми, если же встраивалась пара бит (00) или (11), то строки блока – различны.

Одновременно с формированием блока стеганоконтейнера формируется ключ, который используется на этапе декодирования СИ. Первый элемент ключа соответствует первому блоку стеганоконтейнера, *i*-й элемент – *i*-му блоку. Как было замечено выше, при встраивании (01) или (10) формируются блоки, составленные из одинаковых строк, полученную неоднозначность преодолевают при помощи ключа. Если значение ключа равно 0, то в блок была встроена пара (01), если ключ равен 1, то была встроена пара (10). Аналогично преодолевается неоднозначность и для блоков с различными строками: если значение ключа равно 0, то в блок была встроена пара (00), если ключ равен 1, то была встроена пара (11).

Авторы рассмотренного СА приводят экспериментальные данные, свидетельствующие в пользу устойчивости алгоритма к возмущениям. Однако возмущения моделировались манипулированием наименьшего значащего бита стеганоконтейнера, поэтому такой уровень возмущений только в некоторых случаях может быть достаточным для воспроизведения реальных условий. Более того, реальные возмущения в канале связи, как правило, принято моделировать при помощи гауссовского шума, который аддитивно накладывается на СК. Если учесть специфику стеганопреобразования, после которого строки блока СК должны быть одинаковыми (если встраивались пары бит 01 или 10), то изменение значения любого элемента такого блока даже на единицу приведет к ошибке при декодировании.

Алгоритмом формируется достаточно длинный ключ – он только вдвое меньше длины встраиваемой последовательности, что также требует надежного способа его передачи.

В [5] был предложен стеганографический алгоритм Stego_Graph организации пересылки и декодирования секретной информации, основанный на применении теории графов. Изначально алгоритм разрабатывался для таких информационно-скрывающих систем, где максимизируется скрытая пропускная способность при обеспечении требуемой секретности стегоканала, а к устойчивости к возмущениям предъявляются минимальные требования. Позже Stego_Graph был модифицирован с целью повышения его помехоустойчивости [6].

Идея стеганоалгоритма Stego_Graph состоит в том, чтобы одну бинарную последовательность, выполняющую роль СИ, погрузить в другую бинарную последовательность – контейнер путем сравнения битов СИ с битами контейнера, определяющих в нем в дальнейшем локализацию СИ. В случае несовпадения соответствующих битов СИ и контейнера производится корректировка элементов контейнера с целью приведения их к бинарному виду СИ. Понятно, что для обеспечения требования надежности восприятия СК вычисленное значение его элементов должно находиться в заданных пределах. Так, например, если в качестве контейнера будет использоваться изображение *F*, то вычисленная яркость пикселя $f'(x, y)$ должна удовлетворять условию:

$$f(x, y) - \delta \le f'(x, y) \le f(x, y) + \delta, \qquad (1)$$

где δ – максимально допустимая величина отклонения яркости пикселя от исходного значения.

Из теории обработки изображений известно правило порогового преобразования, приводящее его к бинарному (характеристическому) виду [7]:

$$g(x,y)=\begin{cases}0, \textit{если } f(x,y)\le T,\\ 1, \textit{если } f(x,y)>T\end{cases} \qquad (2)$$

где T – порог, вычисляемый как полусумма максимального и минимального значений пикселей области, для которой он вычисляется.

Стегопреобразование, следуя Stego_Graph, состоит в следующем. СИ, имеющая вид бинарной последовательности, разбивается на подпоследовательности P_i длиною в 8 бит, затем каждая P_i представляется в виде бинарного дерева, для которого строится матрица смежности [7], элементами которой являются нули и единицы. Именно портрет матрицы смежности СИ определяет в дальнейшем ее локализацию в СК. Контейнер-изображение разбивается на блоки F_i размером 8x8, а затем подвергается пороговому преобразованию для приведения его к бинарному виду. Особенностью порогового преобразования блока контейнера-изображения является то, что такое преобразование не всегда можно выполнить, используя глобальный порог, который определяется для всего блока, поскольку, несмотря на сравнительно небольшой размер блока, разность между максимальным и минимальным значением его элементов может составлять большое число. Поэтому, применив (2), как правило, нарушается требование (1). Чтобы избежать подобной ситуации, алгоритм содержит шаг сегментации блока на подобласти, элементы которых лежат в заданных пределах (разность между максимальным и минимальным значением элементов подобласти составляет $2d$), и уж затем каждая подобласть подвергается пороговому преобразованию.

Иллюстрация результата сегментации блока при δ=14 и приведения его к бинарному виду представлена на рис.1. Блок контейнера сегментирован на четыре подобласти со следующей градацией яркостей [214–186], [186–158], [158–130], [130–102] (правая граница не принадлежит области, кроме последней) и соответствующими значениями порогов T_1=200, T_2=172, T_3=144, T_4=116.

213	214	212	197	137	112	110	109
189	210	213	210	165	119	110	108
159	204	210	212	189	137	119	107
133	186	204	209	194	153	128	107
137	175	201	210	195	145	126	107
189	164	175	199	175	131	121	108
214	186	164	154	142	121	113	107
213	200	177	131	119	113	112	106

а

1	1	1	0	0	0	0	0
0	1	1	1	0	1	0	0
0	1	1	1	0	0	1	0
0	1	1	1	0	1	1	0
0	1	1	1	0	1	1	0
0	0	1	0	1	0	1	0
1	1	0	1	0	1	0	0
1	0	1	0	1	0	0	0

б

Рис. 1. Блок 8x8 контейнера-изображения: матрица сегментированного блока (а); результат пороговой обработки блока с учетом сегментации (б)

Более детально остановимся на процессе корректировки яркости пикселя контейнера, которая выполняется в том случае, если его характеристическое

значение (значение соответствующего ему бита) не совпадает со значением бита СИ. Для этого матрицу, изображенную на рис. 1, представим в виде шкалы.

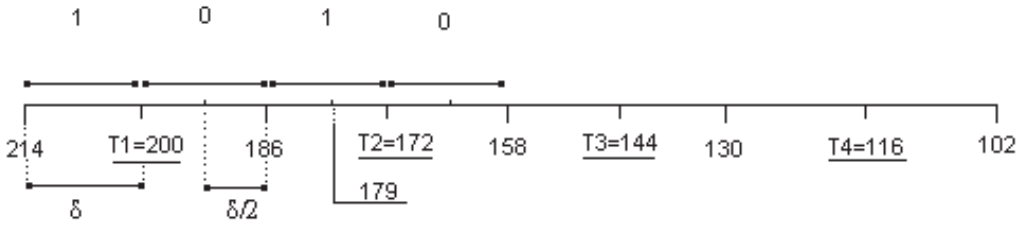

Рис. 2. Блок контейнера в виде шкалы

Если обратиться к рис. 2, то легко заметить, что нули и единицы различных областей чередуются. Для пикселя, характеристическое значение которого равно 1 (кроме первой подобласти), не имеет значения, в какую подобласть он будет переведен, главное при этом сохранить надежность восприятия СК. Например, рассмотрим область со значениями границ [186−158] и порогом $T2=172$. Если пиксель со значением яркости, которое удовлетворяет условию $179=186-\delta/2\le f(x,y)\le 186$, следует изменить так, чтобы его характеристическое значение равнялось нулю, то ему следует присвоить значение $T1-\delta/2=200-7=193$, если же пиксель имеет яркость, удовлетворяющую условию $T2<f(x,y)<T2+\delta/2$, то ему следует присвоить значение $T2-\delta/2=172-7=165$, при этом разность между исходным и новым значением будет удовлетворять условию (1), то есть находиться в пределах $\pm\delta$. Такое стегопреобразование обеспечит устойчивость битов СИ к возмущениям эквивалентных ± 7 градациям яркости.

Модификация Payload Transformation

Алгоритм создания стеганографического контейнера:

Вход: изображение-контейнер (F), СИ в бинарном представлении.

Выход: СК.

1. Разбить контейнер на блоки F_i размером 8x8 каждый.

2. Сегментировать блок F_i на подобласти; вычислить значения порогов T_i для каждой подобласти.

3. Выполнить пороговую обработку F_i для приведения блока к бинарному виду, используя пороги, полученные на предыдущем шаге.

4. Разбить F_i на блоки F_{ij} размером 2x2 каждый.

5. Для текущей битовой пары СИ определить вид матрицы H. Если битовая пара содержит значения (0,0), то $H=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$, для пары (0,1) – $H=\begin{bmatrix}1 & 0\\ 1 & 0\end{bmatrix}$, для пары (1,0) – $H=\begin{bmatrix}0 & 1\\ 0 & 1\end{bmatrix}$, для пары (1,1) – $H=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$.

6. Сравнить H с текущим блоком F_{ij}. В случае несовпадения выполнить корректировку значений элементов контейнера, следуя алгоритму Stego_Graph.

Порядок, в котором матрицы H будут встраиваться в блок F_i, может использоваться как стеганографический ключ, более того, меняя этот порядок, меняется локализация СИ, а СА при этом не требует перестройки.

Алгоритм извлечения СИ из СК:

Вход: СК.
Выход: СИ.

1. Разбить контейнер на блоки F_i размером 8x8 каждый.
2. Сегментировать блок F_i на подобласти; вычислить значения порогов T_i для каждой подобласти.
3. Выполнить пороговую обработку F_i для приведения блока к бинарному виду, используя пороги, полученные на предыдущем шаге.
4. Разбить F_i на блоки F_{ij} размером 2x2 каждый.
5. Выполнить извлечение СИ по правилу: если F_{ij} имеет вид $F_{ij} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, то битовая пара содержит значения (0,0), в случае $F_{ij} = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}$, извлекается пара (0,1), матрице $F_{ij} = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}$ соответствует пара (1,0), а матрице $F_{ij} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ соответствует пара (1,1).

Порядок обработки блоков F_{ij} для извлечения битов СИ соответствует порядку при ее встраивании.

Заключение

В работе разработан новый более устойчивый к возмущениям стеганографический алгоритм, на основе существующего, используя сегментацию блоков контейнера с последующим их пороговым преобразованием. Новый алгоритм по сравнению с базовым, кроме улучшенной помехоустойчивости, не требует формирования ключа, а также использует все блоки контейнера для внедрения СИ, что увеличивает скрытую пропускную способность. Как показали полученные результаты, предварительная сегментация блоков контейнера позволила применить пороговое преобразование и является эффективной предобработкой матрицы при приведении ее к бинарному виду, что может быть использовано для повышения помехоустойчивости СА, аналогичных стеганоалгоритму, рассмотренному в работе, в которых контейнеры могут быть представлены в матричном виде.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. *Fridrich J.* Steganalysis of LSB Encoding in Color Images/ J. Fridrich, R. Du, M. Long // A Proceedings of ICME 2000, New York City, July 31 – August 2, New York, USA.

2. *Husrev T.* Senear Data Hiding Fundamentals And Applications. Content Security In Digital Multimedia / Husrev T. Senear, Mahalingam Ramkumar, Ali N. Akansu // ELSEVIER science and technology books, 2004. – 364 p.

3. *Neil F. Johnson*, Information Hiding : Steganography and Watermarking. – Attacks and Countermeasures / Neil F. Johnson, Zoran Duric, Sushil Jajodia // Kluwer Academic Publishers, 2001. – I60 p.

4. *Shiva Kumar K. B.* Steganography Based on Payload Transformation / K. B. Shiva Kumar, K. B. Raja, R. K. Chhotaray, Sabyasachi Pattnaik // IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 2, March 2011.

5. *Борисенко И.И.* Особенности применения многоуровневого порогового преобразования изображения в компьютерной стеганографии / И.И. Борисенко // Праці УНДІРТ. Теоретичний та науково-практичний журнал радіозв'язку, радіомовлення і телебачення. – 2006. – 4(48). – С. 53–59.

6. *Борисенко И.И.* Повышение помехоустойчивости стеганографического алгоритма / И.И. Борисенко // Сучасний захист інформації. – 2010. – № 1. – С. 36–42.

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

8. *Харари Ф.* Теория графов / Ф. Харари. – М. : Мир, 1973. – 300 с.

Отримано 07.04.2014