УЧЕНЫЕ ЗАПИСКИ КАЗАНСКОГО ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА
Том 149, кн. 2 Физико-математические науки *2007*

УДК 621.391.037.372

СКРЫТАЯ ПЕРЕДАЧА ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ ГРАНИЦ ОБЪЕКТОВ

Е.В. Разинков, Р.Х. Латыпов

Аннотация

В статье предлагается новый метод сокрытия информации в неподвижных изображениях. Основная идея предлагаемого подхода – использование границ объектов для встраивания информации. Предложенный метод сокрытия информации в неподвижных изображениях обеспечивает помехоустойчивость передачи скрытой информации, учет особенностей зрительной системы человека, отсутствие необходимости наличия исходного сигнала для извлечения информации.

1. Введение

Классическая стеганография (с греч. «тайнопись») решает задачи скрытой передачи информации.

Приведем объяснения основных понятий. Контейнер – информационная последовательность, в которой прячется сообщение. Стего – контейнер со встроенной в него информацией. Стегокодер – устройство, предназначенное для встраивания скрываемой информации в контейнер. Стегодекодер – устройство, предназначенное для извлечения скрытой информации из стего.

Евклидово расстояние между векторами $\alpha = (\alpha_1, \ldots, \alpha_p)$ и $\beta = (\beta_1, \ldots, \beta_p)$, α, $\beta \in \mathbf{Z}^p$, обозначим через $d(\alpha, \beta)$:

$$d(\alpha, \beta) = \sqrt{\sum_{i=1}^{p} (\alpha_i - \beta_i)^2}.$$

1.1. Проблема заключенных. Основная задача стеганографии традиционно формулируется в виде «проблемы заключенных» [1] (рис. 1). Канал связи между двумя заключенными, Алисой и Бобом, контролируется стражником Венди. Алиса, пытаясь послать секретное сообщение Бобу, встраивает его в безобидный с точки зрения Венди сигнал-контейнер, в нашем случае – в изображение. Венди, желая помешать секретной передаче информации между Алисой и Бобом, может либо анализировать перехватываемые сообщения на наличие скрытой информации и не пересылать Бобу сообщения, наличие в которых скрытой информации кажется вероятным (Венди – пассивный нарушитель), либо вносить помехи в канал связи, искажая каждое сообщение вне зависимости от его подозрительности в попытках разрушить скрытое сообщение (Венди – активный нарушитель).

Итак, две основные модели нарушителя:

- Пассивный нарушитель. Цель пассивного нарушителя – обнаружение скрытого сообщения. Атаки, доступные пассивному нарушителю (пассивные атаки), – визуальная атака на стего, статистические атаки.
- Активный нарушитель. Цель активного нарушителя – разрушение скрытого сообщения. Атаки, доступные активному нарушителю (активные атаки), – внесение помех в канал связи, искажение стего.

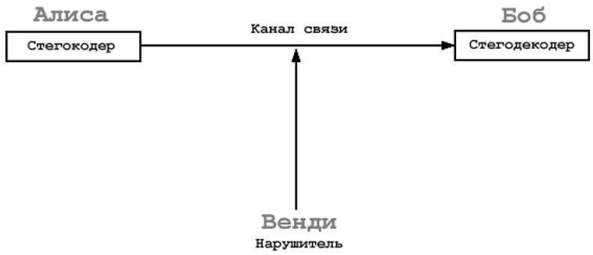


Рис. 1. Проблема заключенных

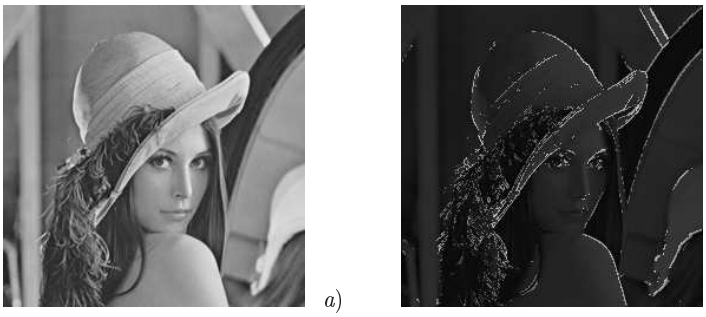
1.2. Понятие стеганографической стойкости. Предполагается, что нарушителю известны используемые в стегосистеме алгоритмы встраивания и извлечения скрываемой информации, распределения/вероятностные модели контейнеров, скрываемых сообщений, стего, стеганографических ключей. Стегосистема считается стойкой к пассивной стегоаналитической атаке, если нарушитель, обладая одним или несколькими перехваченными стего, но не зная секретного стеганографического ключа, не способен делать выводы о наличии или отсутствии в стего скрытой информации.

Стойкость стегосистемы скрытой передачи данных определяется ее стойкостью к пассивным стегоаналитическим атакам.

1.3. Классификация стегосистем. Стегосистемы различают по [2]:

- выполняемой задаче:
  - стегосистемы скрытой передачи данных,
  - стегосистемы цифровых водяных знаков,
  - прочие;
- природе сигнала, используемого в качестве контейнера:
  - аналоговая природа сигнала,
  - цифровая природа сигнала;
- необходимости наличия у стегодетектора исходного сигнала:
  - для извлечения встроенной информации требуется исходный сигнал,
  - для извлечения встроенной информации исходного сигнала не требуется;
- типу присутствующего нарушителя:
  - пассивный нарушитель,
  - активный нарушитель.

В данной работе мы предлагаем подход к созданию стегосистемы скрытой передачи данных, использующей в качестве стегоконтейнера сигнал, полученный в результате оцифровки аналогового сигнала. Предполагается наличие пассивного нарушителя.



а) *б*)

Рис. 2. *а*) Стеганографический контейнер; *б*) множество элементов контейнера, удовлетворяющих базовым критериям

2. Модель сигнала

Предложим модель сигнала, в который встраивается информация. В качестве стегоконтейнера рассмотрим функцию $f : C \to X$, где

$$C \subset \mathbf{Z}^2, \quad C = \{(c_1, c_2) | a_1 \le c_1 \le b_1, \quad a_2 \le c_2 \le b_2, \quad c_1, c_2 \in \mathbf{Z}\},$$

$$X \subset \mathbf{Z}^m, \quad X = \{(x_1, x_2, \ldots, x_m) | u_j \le x_j \le v_j, \quad x_j \in \mathbf{Z}, \quad j = 1, \ldots, m\}.$$

Вектор $c \in C$ назовем элементом стегоконтейнера f, а вектор $x = f(c)$, $c \in C$, $x \in X$, – значением элемента c.

Элементы множества $H_c = \{\bar{c} | \bar{c} \in C, d(c, \bar{c}) = 1\}$ будем называть соседними элементами контейнера по отношению к элементу c.

3. Предлагаемый подход

Основная идея предлагаемого подхода – использование границ объектов для встраивания скрываемой информации (рис. 2, *а*).

Под границами объектов будем понимать элементы множества $B_f^L \subset C$:

$$B_f^L = \Big\{ c | c \in C, \exists z_1, z_2, z_3, z_4 \ge 0, \\ \sum_{i=1}^{4} z_i = 1 : f(c) = f(c_1, c_2) = z_1 f(c_1 + 1, c_2) + z_2 f(c_1 - 1, c_2) + \\ + z_3 f(c_1, c_2 + 1) + z_4 f(c_1, c_2 - 1); \\ \min_{\bar{c} \in H_c} d(f(c), f(\bar{c})) \ge L, L \ge 0 \Big\}.$$

В качестве пояснения приведем критерии выбора элементов стегоконтейнера для включения в множество B_f^L. Назовем эти критерии базовыми (рис. 2, *б*). Базовые критерии выбора элементов контейнера для встраивания информации:

- значение элемента контейнера должно быть выпуклой комбинацией значений соседних элементов;
- расстояние от значения элемента контейнера до значений соседних элементов должно быть не меньше некоторого заданного порога L.

Правило изменения элементов стегоконтейнера задается следующим образом: каждому $c \in B_f^L$ ставится в соответствие множество $M_f^c \subset X$ допустимых результатов изменения значения c:

$$M_f^c = \{\bar{x} \in X | \ \forall I_1, I_2, I_3, I_4 \in \{0,1\} : \ \exists z_1, z_2, z_3, z_4 \geq 0,$$
$$\sum_{i=1}^{4} z_i = 1, \quad f(c) = I_1 z_1 f(c_1+1, c_2) + I_2 z_2 f(c_1-1, c_2) +$$
$$+ I_3 z_3 f(c_1, c_2+1) + I_4 z_4 f(c_1, c_2-1) \Rightarrow \exists \bar{z}_1, \bar{z}_2, \bar{z}_3, \bar{z}_4 \geq 0,$$
$$\sum_{i=1}^{4} \bar{z}_i = 1 : \ \bar{x} = I_1 \bar{z}_1 f(c_1+1, c_2) + I_2 \bar{z}_2 f(c_1-1, c_2) +$$
$$+ I_3 \bar{z}_3 f(c_1, c_2+1) + I_4 \bar{z}_4 f(c_1, c_2-1); \quad \min_{\bar{c} \in H_c} d(\bar{x}, f(\bar{c})) \geq L\}.$$

Базовые критерии определения возможного изменения значения элемента стегоконтейнера:

- Для любого набора соседних элементов, выпуклой комбинацией значений которых являлось значение рассматриваемого элемента стегоконтейнера, оно должно оставаться выпуклой комбинацией их значений.
- Расстояние от значения элемента после изменения до значений соседних элементов не должно быть меньше L.

Пример. Рассмотрим случай цветного изображения: $m = 3$. Выпуклая оболочка значений пикселов c^1, c^2, c^3 и c^4 в общем случае представляет собой тетраэдр с вершинами в точках $f(c^1)$, $f(c^2)$, $f(c^3)$ и $f(c^4)$. Таким образом, значение пиксела c удовлетворяет первому базовому критерию, если значение $x = f(c)$ этого пиксела лежит внутри тетраэдра с вершинами в точках $f(c^1)$, $f(c^2)$, $f(c^3)$, $f(c^4)$.

3.1. Дополнительные критерии. В зависимости от требуемых свойств стегосистемы выбираются дополнительные критерии и ограничения, задается значение параметра L.

Определим требования к дополнительным критериям построения множества элементов контейнера, подходящих для встраивания информации, и к построению правила изменения элементов контейнера.

Для каждого $c \in B_f^L$ построим множество функций:

$$\bar{F}_c = \{\bar{f} | \bar{f}(\bar{c}) = f(\bar{c}), \quad \bar{c} \neq c; \quad \bar{f}(\bar{c}) \in M_f^c, \quad \bar{c} = c; \quad \bar{c}, c \in C\}.$$

Очевидно, что $f \in F_c$ для любого $c \in B_f^L$.

Условия, накладываемые на множество $\bar{K}_f^L$ и правило изменения $\bar{M}$ и построенные на основе дополнительных критериев:

- $\bar{K}_f^L \subset B_f^L$,
- $f(c) \in \bar{M}_f^L \forall c \in \bar{K}_f^L$,
- $\bar{M}_f^c \subset M_f^c \forall c \in \bar{K}_f^L$,
- $c \in \bar{K}_{\tilde{f}}^L, \bar{f} \in \bar{F}_c \Rightarrow c \in \bar{K}_{\tilde{f}}^L \forall \tilde{f} \in \bar{F}_c, \forall c \in B_f^L$.

Скрывающее преобразование, построенное с учетом критериев, удовлетворяющих этим условиям, не нарушает синхронизации стегокодера и стегодекодера.

В дальнейшем будем обозначать через K_f^L множество элементов контейнера, подходящих для встраивания информации, вне зависимости от того, было ли это множество построено с учетом лишь базовых критериев или с учетом и базовых, и дополнительных критериев.

3.2. Множество G. Для того чтобы скрытое сообщение могло быть корректно извлечено из стего и синхронизация стегокодера и стегодекодера не нарушалась при отсутствии у адресата неизмененного стегоконтейнера, не все элементы контейнера из множества K_f^L подвергаются модификации. Задается некоторое множество $G \subset C$, и только принадлежащие этому множеству элементы контейнера могут быть модифицированы в случае выполнения базовых критериев. Необходимо задать правило построения множества G, удовлетворяющее следующему условию:

$$c, \bar{c} \in K_f^L \cap G \Rightarrow d(c, \bar{c}) \neq 1.$$

Среди элементов стегоконтенера, удовлетворяющих базовым критериям и входящих в G, не должно быть соседних.

При построении помехоустойчивой стегосистемы критически важным может оказаться дополнительное ограничение, накладываемое на правило построения множества G:

$$c, \bar{c} \in G \Rightarrow d(c, \bar{c}) \neq 1.$$

Включение элемента стегоконтейнера в множество G зависит только от положения этого элемента в контейнере и не зависит от его значения или значений других элементов.

Зафиксируем некоторое множество $I \in \{0, 1\}$. Следующий способ построения G удовлетворяет последнему свойству:

$$G_I = \{c = (c_1, c_2) | c_1 + c_2 \equiv I \pmod 2\}.$$

В множество G включаются те элементы стегоконтейнера, сумма координат которых четна (нечетна).

3.3. Стеганографический ключ. В рамках предлагаемого метода значения не всех элементов множества $K_f^L \cap G$ подвергаются модификации, но в соответствии со стеганографическим ключом k – секретной информацией, известной участникам скрытого информационного обмена. Множество элементов из $K_f^L \cap G$, подлежащих модификации в соответствии с ключом k, обозначим через $D^k_{K_f^L \cap G}$.Стеганографический ключ используется при встраивании информации в контейнер и при извлечении информации из стего.

3.4. Скрывающее преобразование. Результатом применения скрывающего преобразования является стего.

Процедуру применения скрывающего преобразования можно разбить на следующие этапы:

- построение множества K_f^L в соответствии с базовыми и дополнительными критериями;
- построение множества G;

- определение в соответствии со стеганографическим ключом тех элементов стегоконтейнера из множества $K_f^L \cap G$, значения которых будут изменены при встраивании информации;
- встраивание информации – модификация значений элементов контейнера в соответствии с правилом изменения значений элементов контейнера.

3.5. Извлечение информации. Если стего не было искажено при передаче, элементы стего, значения которых содержат скрытую информацию, определяются с помощью тех же критериев и того же стеганографического ключа, что использовались при встраивании информации.

4. Сокрытие информации в полутоновых изображениях

Рассмотрим частный случай стегоконтейнера – полутоновое изображение: $m = 1$. Элементы изображения $c \in C$ будем называть пикселами, значением пиксела будем называть его яркость, выраженную целым числом x, $u_1 = 0$, $v_1 = 255$.

Диапазон изменения, определяемый базовыми критериями, будем называть базовым диапазоном изменения, а его нижнюю и верхнюю границы – нижней и верхней базовой границей соответственно.

Известно, что зрительная система человека слабо чувствительна к искажениям вблизи границ объектов [3].

4.1. Использование метода вместе с методом LSB. Существует метод сокрытия информации в изображениях путем модификации наименее значащего бита (далее – метод LSB, от “Least Significant Bit” (англ.) – наименее значащий бит) [4]. Информация встраивается в изображение путем модификации наименее значащего бита (иногда двух младших бит) байта, которым кодируется либо яркость каждого пиксела (полутоновое изображение), либо каждая из трех цветовых компонент пиксела (цветное изображение). Метод LSB имеет очень высокую пропускную способность канала передачи скрываемой информации, но является неустойчивым к стегоаналитическим атакам, а самое незначительное изменение стего разрушает скрытое сообщение [5]. Существуют модификации этого метода, направленные на повышение устойчивости к пассивным стегоаналитическим атакам, однако пропускная способность скрытого канала передачи информации в этих модификациях значительно ниже.

Предлагаемый нами метод может быть использован вместе с методом LSB. Использование LSB оправдано, если предполагается отсутствие шума в канале связи и отсутствие сжатия изображения с потерями.

Корректность работы предлагаемого метода при использовании его вместе с методом LSB обеспечивается достижимостью отсутствия влияния младших бит значений пикселов на процессы встраивания информации в контейнер и извлечения информации из стего. После применения с такими ограничениями предлагаемого метода используется метод LSB.

4.2. Обеспечение помехоустойчивости. Предлагаемый метод может обеспечивать скрытый информационный обмен и при наличии аддитивного шума, который изменяет значение каждого пиксела не более, чем на некоторую величину h. Предполагается, что значение h известно как скрывающему информацию, так и получателю сообщения.

Корректность передачи скрываемой информации при наличии аддитивного шума обеспечивается выполнением двух условий:

- присутствующий шум не должен изменять множество $K_f^L \cap G$;
- если значение пиксела изображения было изменено скрывающим преобразованием при встраивании бита сообщения, то влияние шума на значение этого пиксела не должно привести к несовпадению встроенного и извлеченного значений бита скрытого сообщения.

При построении помехоустойчивой стегосистемы базовые критерии выбора пикселов дополняются еще одним критерием – требованием к базовому интервалу изменения: базовый интервал изменения должен быть не меньше, чем некоторая величина S.

Множество пикселов, построенное с учетом этого критерия, обозначим через $K^{L,S}$. В результате воздействия шума базовый интервал изменения значения пиксела не может измениться на величину, большую чем $2h$. Таким образом, если информация встраивалась в пикселы с базовым диапазоном S и выше, то при извлечении информации из стего необходимо анализировать пикселы, начиная с базового диапазона $S - 2h$. Очевидно, в это множество попадут и пикселы, базовые диапазоны изменения которых до воздействия шума были меньше S, но больше $S - 4h$, то есть те, в которые информация не встраивалась. Для того чтобы исключить их из рассмотрения и не допустить изменения множества $K^{L,S}$, значение каждого из этих пикселов изменяется и устанавливается равным либо нижней базовой границе, либо верхней, в зависимости от того, какая из них ближе к значению пиксела.

В результате воздействия шума расстояние между двумя значениями пикселов может измениться на величину, не превышающую $2h$. Поэтому при извлечении информации из стего при проверке выполнения второго базового критерия следует использовать параметр $L = L_0 + 2h$, где L_0 – соответствующий параметр скрывающего преобразования. Значения пикселов, в которые была встроена информация, после применения скрывающего преобразования и воздействия шума должны удовлетворять, в частности, второму базовому критерию с параметром L. При извлечении информации значение извлекаемого бита определяется в зависимости от того, по какую сторону от середины базового диапазона лежит значение анализируемого пиксела. Из всего вышесказанного следует, что значение пиксела c^i при встраивании бита сообщения следует изменить следующим образом: если значение встраиваемого бита равно 0, то новое значение пиксела должно принадлежать интервалу

$$(m_i + L_0 + 4h; (m_i + M_i)/2 - 2h),$$

если значение бита равно 1, то новое значение пиксела должно принадлежать интервалу

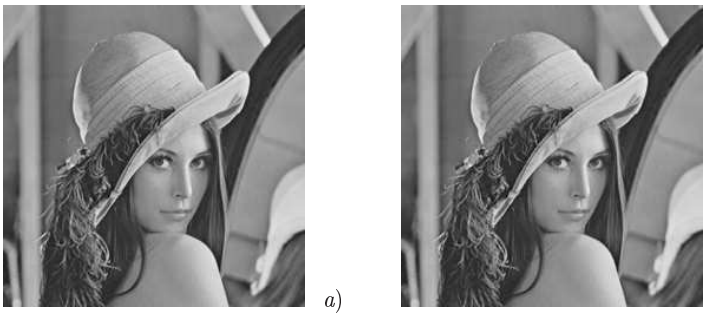
$$((m_i + M_i)/2 + 2h; M_i - L_0 - 4h),$$

где m_i и M_i – нижняя и верхняя базовые границы диапазона изменения значения пиксела c^i соответственно .

4.3. Повышение стеганографической стойкости и визуальной незаметности. Повышению стойкости стегосистемы к статистической атаке и повышению визуальной незаметности искажения, вносимого скрывающим преобразованием, способствует сокращение диапазона изменения значений пикселов.

Пусть m и M – нижняя и верхняя базовые границы диапазона изменения значения $x = f(c)$ некоторого пиксела c соответственно. Заметим, что

$$(x + m)/2 < (m + M)/2 < (x + M)/2.$$



а) *б*)

Рис. 3. Демонстрация применения метода: *а*) исходное изображение; *б*) стего

При встраивании информации новое значение пиксела определяется следующим образом: если значение встраиваемого бита сообщения равно 0, то значение пиксела c выбирается из интервала:

$$((x+m)/2; (m+M)/2),$$

если значение встраиваемого бита равно 1, то новое значение выбирается из интервала:

$$((m+M)/2; (x+M)/2).$$

При извлечении информации вывод о значении извлекаемого бита делается в зависимости от того, по какую сторону от середины базового диапазона лежит значение анализируемого пиксела (рис. 3, *а*, *б*).

4.4. Пропускная способность скрытого канала. При встраивании в пиксел не более чем одного бита количество информации, которое можно встроить в изображение, ограничено величиной $|K_f^L \cap G|$.

При определенных условиях появляется возможность встраивания более чем одного бита сообщения в значение пиксела. В этом случае количество информации, которое можно встроить в изображение, не превышает значения

$$\sum_{i=1}^{|K_f^L \cap G|} [\log_2 S_i],$$

где S_i – длина базового интервала изменения значения i-го пиксела из множества $K_f \cap G$.

4.5. Возможные атаки. Для оценки стойкости стегосистемы к атакам пассивного нарушителя предложим подход к построению пассивной атаки, направленной на выявление наличия скрытого сообщения. Предположим, что нарушитель обладает одним экземпляром стего и осведомлен о параметрах скрывающего преобразования. Таким образом, ему известно множество пикселов изображения, которые могли быть подвергнуты модификации.

Каждый пиксел изображения будем интерпретировать как реализацию случайной величины, зависимой от соседних пикселов. Это предположение вполне естественно и позволяет поставить в соответствие каждому пикселу некоторую случайную величину Y_θ, равную разности случайной величины значения этого пиксела и прогноза его значения, сделанного на основе знания значений соседних пикселов. Заметим, что случайная величина Y_θ зависит от параметра θ, описывающего соотношение между значениями соседних пикселов, возможными значениями

оцениваемого пиксела (знание параметров стегосистемы и скрывающего преобразования дает нарушителю информацию о множестве значений случайной величины значения для каждого пиксела).

Зафиксируем некоторое значение параметра θ. Стегоаналитик, располагая перехваченным изображением, имеет набор реализаций случайной величины Y_θ. Проведенный нами анализ распределения Y_θ при фиксированном параметре θ показывает, что применение построенного с использованием предлагаемого нами подхода скрывающего преобразования с определенными параметрами преобразования влечет изменение параметров распределения Y_θ, заключающееся в изменении дисперсии распределения. Это дает стегоаналитику возможность, при достаточном количестве перехваченных стего, делать некоторые предположения о наличии/отсутствии в них скрытой информации.

Сложность проведения пассивной стегоаналитической атаки обусловлена:

- возможностью применения скрывающего преобразования с параметрами, минимизирующими изменение дисперсии и других статистических характеристик изображения, при незначительном снижении пропускной способности канала скрытой передачи данных;
- недостаточным количеством информации о распределении Y_θ для фиксированного параметра θ, что обусловлено областью значений параметра.

4.6. Достоинства и недостатки стегосистемы.

Достоинства:

- Сложность проведения противником пассивных статистических атак, неприменимость существующих атак.
- Помехоустойчивость. Скрытый канал связи устойчив к незначительному аддитивному шуму при известной вероятностной модели шума.
- Достижима устойчивость к JPEG-компрессии, сохраняющей высокий уровень качества изображения.
- Отсутствие необходимости наличия у адресата исходного изображения.
- Учет особенностей зрительной системы человека.
- Возможность использования предлагаемого метода совместно с методом LSB. В случае, когда высокая пропускная способность важнее устойчивости к аддитивному шуму, предлагаемый нами метод может быть использован совместно с методом LSB.
- Невысокая вычислительная сложность. Это свойство расширяет область возможного применения стегосистемы. Например, стегокодер и стегодекодер поточной стегосистемы должны обладать невысокой вычислительной сложностью.

Недостатки:

- Невысокая пропускная способность.

5. Заключение

Предстоит тщательный анализ устойчивости метода: построение возможных стегоаналитических атак и выработка мер по противодействию им. Вызывает интерес возможность применения предложенного подхода при сокрытии информации в видеопоследовательностях.

Summary

E.V. Razinkov, R.Kh. Latypov. Data hiding technique using objects outlines.

In this paper we propose a new steganography technique. The main concept of the proposed approach lies in use of objects outlines to hide information. The proposed technique is based on aspects of human visual system, provides noise immunity of subliminal channel, complexity of effective passive steganalysis attacks building, low computational complexity, possibility of secret message extraction in case of absence of unmodified cover message.

Литература

1. *Chandramouli R.* Mathematical approach to steganalysis // Proceedings of the SPIE Security and Watermarking of Multimedia Contents IV, V. 4675. International Society for Optical Engineering, San Jose, California, January 21–24, 2002. – California, 2002. – P. 14–25.
2. *Husrev T. Sencar, Mahalingam Ramkumar, Ali N. Akansu* Data hiding fundamentals and applications. – Elsevier Academic Press, 2004. – 256 с.
3. *Грибунин В.Г., Оков И.Н., Туринцев И.В.* Цифровая стеганография. – М.: СОЛОН-Пресс, 2002. – 272 с.
4. *Rao C.R., Wegman E.J., Solka J.L.* Handbook of statistics. V. 24. Data mining and data visualization. – Elsevier North Holland, 2005. – 646 с.
5. *Конахович Г.Ф., Пузыренко А.Ю.* Компьютерная стеганография. Теория и практика. – Киев: МК-Пресс, 2006. – 288 с.

Поступила в редакцию
23.08.07

Разинков Евгений Викторович – аспирант кафедры системного анализа и информационных технологий Казанского государственного университета.

E-mail: *Razinkov@steganography.ru*

Латыпов Рустам Хафизович – доктор технических наук, профессор, декан факультета вычислительной математики и кибернетики Казанского государственного университета.

E-mail: *Roustam.Latypov@ksu.ru*