Разработка модели стегоконтейнера и методов анализа и повышения стойкости стеганографических систем

Разинков Е.В.

Казанский федеральный университет

План доклада

- Цели исследования
- Актуальность исследования
- Научная новизна
- Описание модели стегоконтейнера
- Описание методов повышения стойкости или пропускной способности
- Полученные результаты
- Апробация работы
- Публикации

Цели исследования

- **Цели исследования:**
  - **Изучение факторов, влияющих на стойкость стегосистем к определенным атакам**
  - **Постановка задачи оптимального распределения встраиваемой информации**
  - **Разработка математической модели стеганографического контейнера**
  - **Разработка метода и соответствующих алгоритмов решения поставленной задачи, обеспечивающих:**
    - **Повышение стойкости и/или пропускной способности стегосистемы к существующим стегоаналитическим атакам**
  - **Разработка программного обеспечения, реализующего метод**

Актуальность исследования

- Развитие сети Интернет открывает широкие возможности использования цифровой стеганографии.
- Ключевые характеристики стеганографической системы:
  - Стойкость
  - Пропускная способность
- Повышение стойкости при малых размерах встроенного сообщения имеет особое значение
- JPEG – распространенный формат изображений

Научная новизна

Существующие способы повышения стойкости или пропускной способности стегосистем:

- Матричное встраивание – способ повышения эффективности встраивания
- Использование дополнительной информации при встраивании (стеганография с нарушением квантования, метод MME)

Пакетная стеганография (A. Кер) исследует оптимальное распределение информации между различными контейнерами. Особенности:

- Предполагается, что различные контейнеры схожи по своим свойствам
- Очевидное отсутствие корреляции между контейнерами

Научная новизна

На защиту выносятся:

- **Модель стегоконтейнера и метод повышения стойкости и/или пропускной способности стеганографических систем за счет оптимального выбора элементов контейнера в скрывающем преобразовании.**

- **Метод выбора элементов контейнера, обеспечивающий абсолютную стойкость к RS-стегоанализу**

- **Модификация метода встраивания информации в изображение с использованием комплексного преобразования Адамара, направленная на повышение стойкости к активному стегоанализу**

Стеганографическая стойкость

Рассмотрим теоретико-информационное определение стеганографической стойкости, использующее понятие относительной энтропии.

Пусть *c* – элемент множества возможных контейнеров/стего.

$P_C(c)$ **– вероятность того, что будет выбран контейнер *c*.**

$P_S(c)$ **– вероятность того, что будет сгенерировано стего *c*.**

Относительная энтропия:

$$D(P_c \| P_s) = \sum_{c \in C} P_C(c) \log \frac{P_C(c)}{P_S(c)}$$

Стеганографическая стойкость

Пусть α и β – вероятности ошибок обнаружения первого и второго рода.

Тогда

$$\alpha \log \frac{\alpha}{1-\beta} + (1-\alpha)\log \frac{1-\alpha}{\beta} \le D(P_C \,\|\, P_S)$$

Пусть $D(P_C||P_S) = \varepsilon$. **Если** $\alpha = 0$,

$$\beta \ge 2^{-\varepsilon}$$

Стеганографическая стойкость

Пусть $\mathbf{v}(c)$ **– вектор характеристик контейнера** c.

Тогда $D(P_C(\mathbf{v}(c))||P_S(\mathbf{v}(c)))$ **характеризует стойкость стегосистемы к атакам, использующим набор характеристик v.**

$$D\left(P_C\left(\mathbf{v}\left(c\right)\right)\|\,P_S\left(\mathbf{v}\left(c\right)\right)\right)\leq D\left(P_C\left(c\right)\|\,P_S\left(c\right)\right)$$

Виды стегоанализа

Виды пассивного стегоанализа:

- **Универсальный, «слепой» стегоанализ**
  - **Набор характеристик PEV-274**
- **Статистический стегоанализ**
  - **RS-стегоанализ**

Набор характеристик PEV-274

PEV-274 включает 274 характеристики, учитывающие:

- Общую гистограмму и гистограммы коэффициентов для каждой группы (165 характеристик)
- Корреляцию между коэффициентами одного блока (81 характеристика)
- Корреляцию между коэффициентами соседних блоков (26 характеристик)
- Блочность изображения (2 характеристики)

RS-стегоанализ

$G = (x_1, \ldots, x_n)$ – **группа пикселей**

Мера гладкости:

$$g(x_1,\ldots,x_n) = \sum_{i=1}^{n-1} |x_{i+1} - x_i|$$

F_1: $0 \leftrightarrow 1$, $2 \leftrightarrow 3$, $4 \leftrightarrow 5$, …, $254 \leftrightarrow 255$.

F_{-1}: $-1 \leftrightarrow 0$, $1 \leftrightarrow 2$, …, $253 \leftrightarrow 254$, $255 \leftrightarrow 256$.

F_0: $0 \leftrightarrow 0$, $1 \leftrightarrow 1$, $2 \leftrightarrow 2$, …, $255 \leftrightarrow 255$.

Маска $M = \{m_i\}$, $i = 1, \ldots, n$

$$F(G) = \left(F_{m_1}(x_1),\ldots,F_{m_n}(x_n)\right)$$

RS-стегоанализ

R_M: $g(F(G)) > g(G)$ – **регулярные группы**

S_M: $g(F(G)) < g(G)$ – **сингулярные группы**

U_M: $g(F(G)) = g(G)$ – **константные группы**

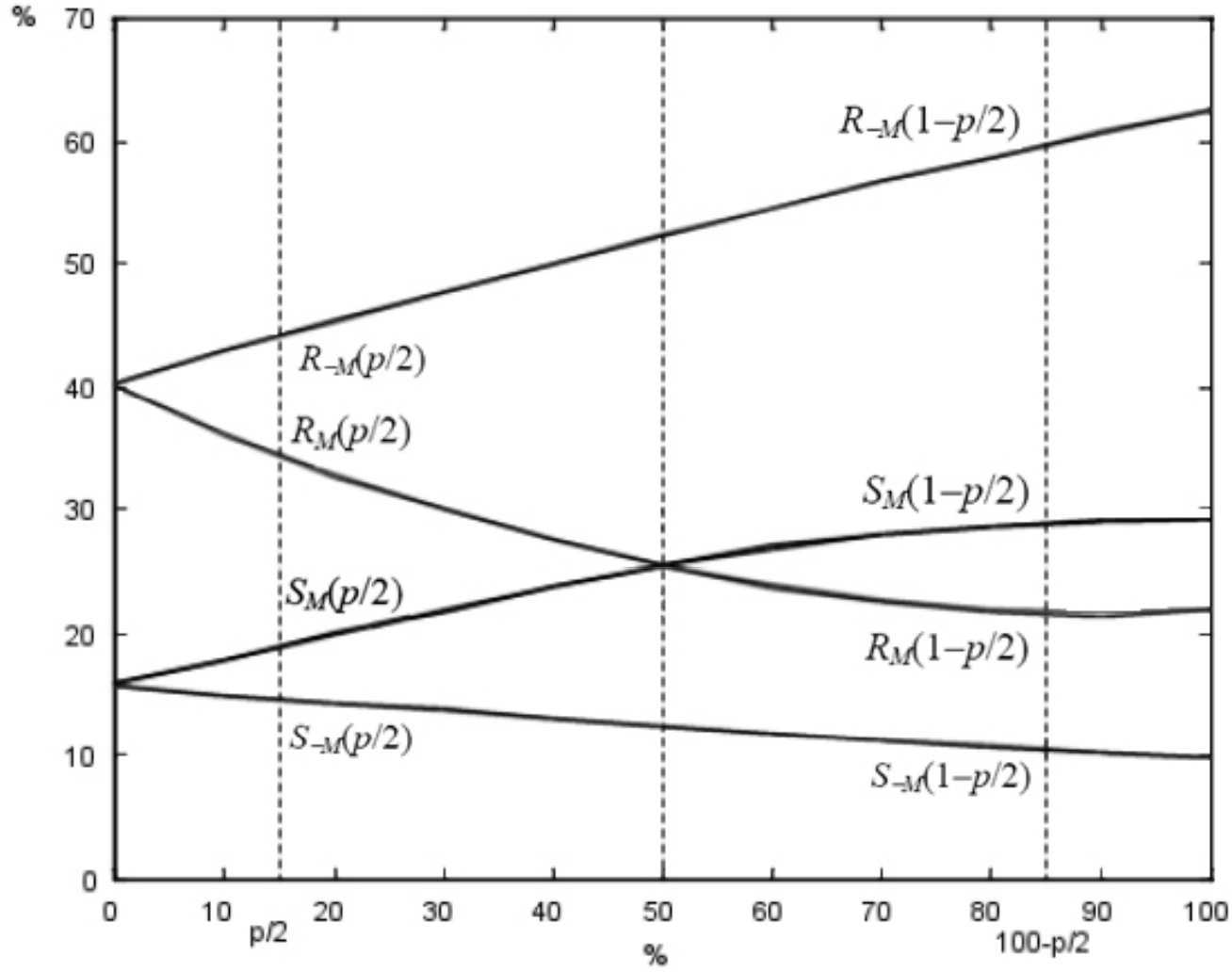
Выдвигается гипотеза, что в случае контейнера без встроенной информации выполняется:

$$R_M \approx R_{-M}$$

$$S_M \approx S_{-M}$$

Справедливость гипотезы подтверждена экспериментально

RS-стегоанализ



Устойчивость к RS-стегоанализу

Базовые критерии выбора пикселей для встраивания информации:

- Значение пикселя должно быть выпуклой комбинацией значений соседних пикселей
- Расстояние от значения пикселя до значений соседних пикселей должно быть не меньше некоторого заданного порога.

Базовые критерии выбора диапазона допустимого изменения значения пикселя:

- После изменения значение пикселя должно удовлетворять базовым критериям выборы пикселей

Встраивание информации с использованием границ объектов

Оригинальное изображение

Используемые пиксели

Модель стегосистемы

- Объединим элементы стеганографического контейнера, подходящие для встраивания информации, на непересекающиеся группы так, что элементы контейнера, объединенные в одну группу, имеют одинаковые или схожие свойства и, как минимум, имеют одинаковое распределение.

- Пример: 63 группы AC-коэффициентов JPEG-преобразования.

Модель стегосистемы

Стеганографический контейнер рассматривается нами как m групп своих элементов, каждая из которых описывается:

- функцией распределения
- количеством элементов
- количеством элементов, которые могут быть модифицированы.

При определении стойкости стегосистемы и вычислениии относительной энтропии, мы будем рассматривать свойства цифрового объекта, которые лежат в основе стегоаналитических атак:

- Распределение элементов в группе
- Корреляция между элементами одной группы
- Корреляция между элементами разных групп

Модель стегосистемы

$f_u(c)$ – функция плотности распределения элементов ***u*-ой группы.**

x_u – количество элементов ***u*-ой группы,** модифицируемых скрывающим преобразованием.

$\bar{f}_u(c, x_u)$ – функция плотности распределения элементов u-ой группы после модификации x_u элементов.

Мы предполагаем, что встраиваемое сообщение имеет максимальную энтропию, так как оно сжато и/или зашифровано.

Модель стегосистемы

Если в качестве контейнера используется изображение в формате JPEG ($c \neq 0$) **:**

$$\bar{f}_u(c, x_u) = \frac{k_u - x_u}{k_u} f_i(c) + \frac{x_u}{k_u}\left(f_u(c) + f_u(c + \operatorname{sgn}(c))\right)$$

Относительная энтропия:

$$D_1\left(P_C \,\|\, P_S(\mathbf{x})\right) = \sum_u k_u \sum_c f_u(c) \log_2 \frac{f_u(c)}{\bar{f}_u(c, x_u)}$$

Модель стегосистемы

$P_u(c,d)$ **- матрица переходных вероятностей цепи Маркова для неизмененного контейнера.**

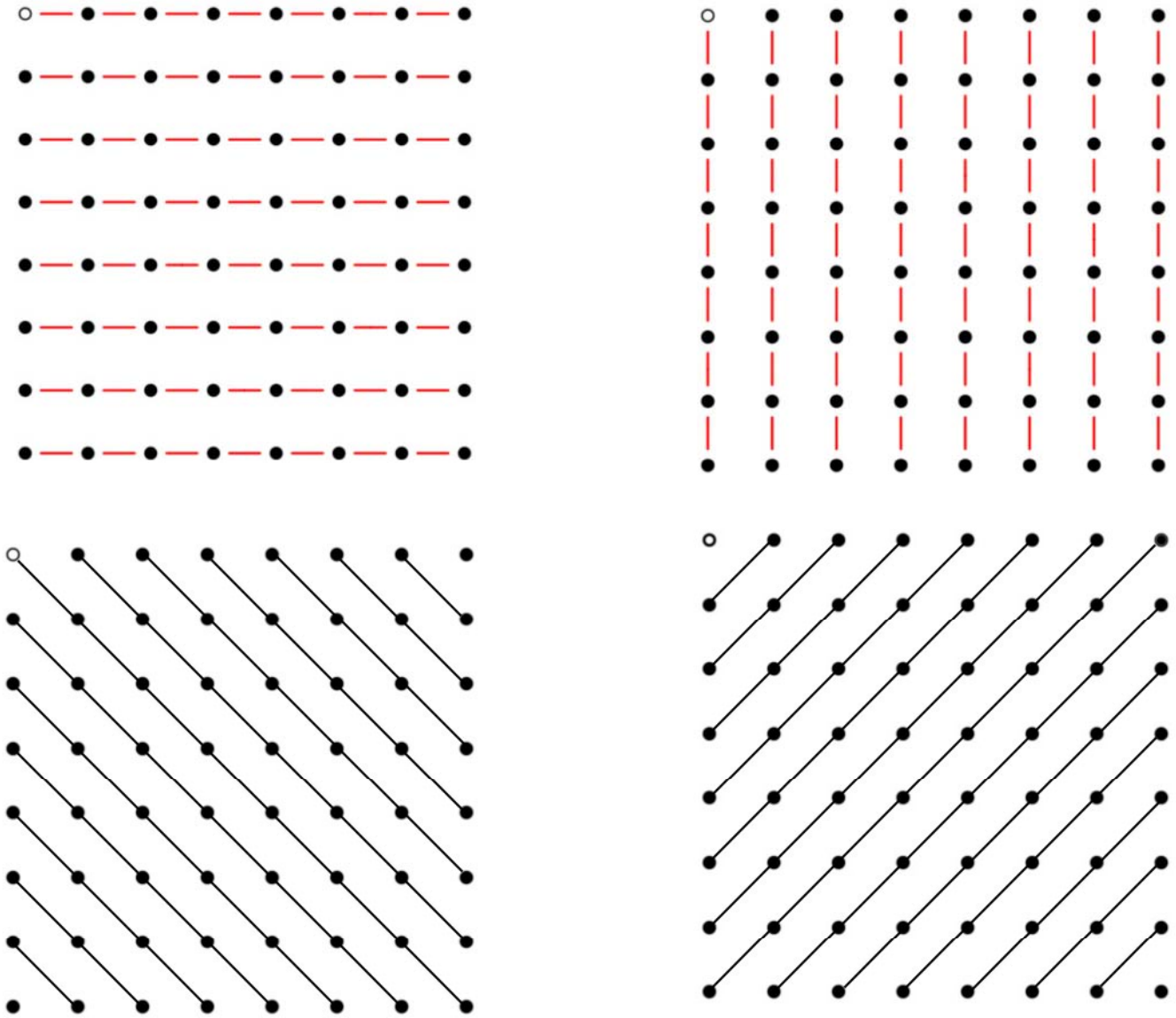
$$\overline{P_u}(c,d,x_u)=\frac{(1-p)^2 P_u^*(c,d)+p(1-p)\left(P_u^*(c+1,d)+P_u^*(c,d+1)\right)+p^2 P_u^*(c+1,d+1)}{\overline{f_u}(c,x_u)}$$

$$p=\frac{x_u}{2k_u};\quad P_u^*(c,d)=P_u(c,d)f_u(c);\ c>0,d>0$$

Относительная энтропия:

$$D_2\left(P_C \,\|\, P_S(\mathbf{x})\right)=\sum_u k_u \sum_{c,d} P_u(c,d)f_u(c)\log_2\frac{P_u(c,d)}{\overline{P_u}(c,d,x_u)}$$

Корреляция между JPEG-коэффициентами



Модель стегосистемы

$P_{uv}(c,d)$ **- матрица переходных вероятностей цепи Маркова для неизмененного контейнера.**

$\overline{P_{uv}}(c,d,x_u,x_v)$ **- матрица переходных вероятностей для стего**

Относительная энтропия:

$$D_3\left(P_C \,\|\, P_S(\mathbf{x})\right) = \sum_{(u,v)\in Corr} k_u \sum_{c,d} P_{uv}(c,d) f_u(c) \log_2 \frac{P_{uv}(c,d)}{\overline{P_{uv}}(c,d,x_u,x_v)}$$

Постановка задачи

Для заданного n, векторов k, k* и функций D_1, D_2 и D_3 найти вектор x = $\{x_u\}$ такой, что

$$D\left(P_C \,\|\, P_S\left(\mathbf{x}\right)\right) = D_1\left(\mathbf{x}\right) + D_2\left(\mathbf{x}\right) + D_3\left(\mathbf{x}\right) \to \min$$

$$\sum_u x_u = n$$

$$0 \le x_u \le k_u^* \le k_u, \; u = \overline{1, m}$$

Некоторые утверждения

Поставленная задача обладает следующими свойствами:

1. Пусть x – решение задачи с параметрами (*n*, k, k*). Тогда *γ*x – решение аналогичной задачи с параметрами (*γn*, *γ*k, *γ*k*).

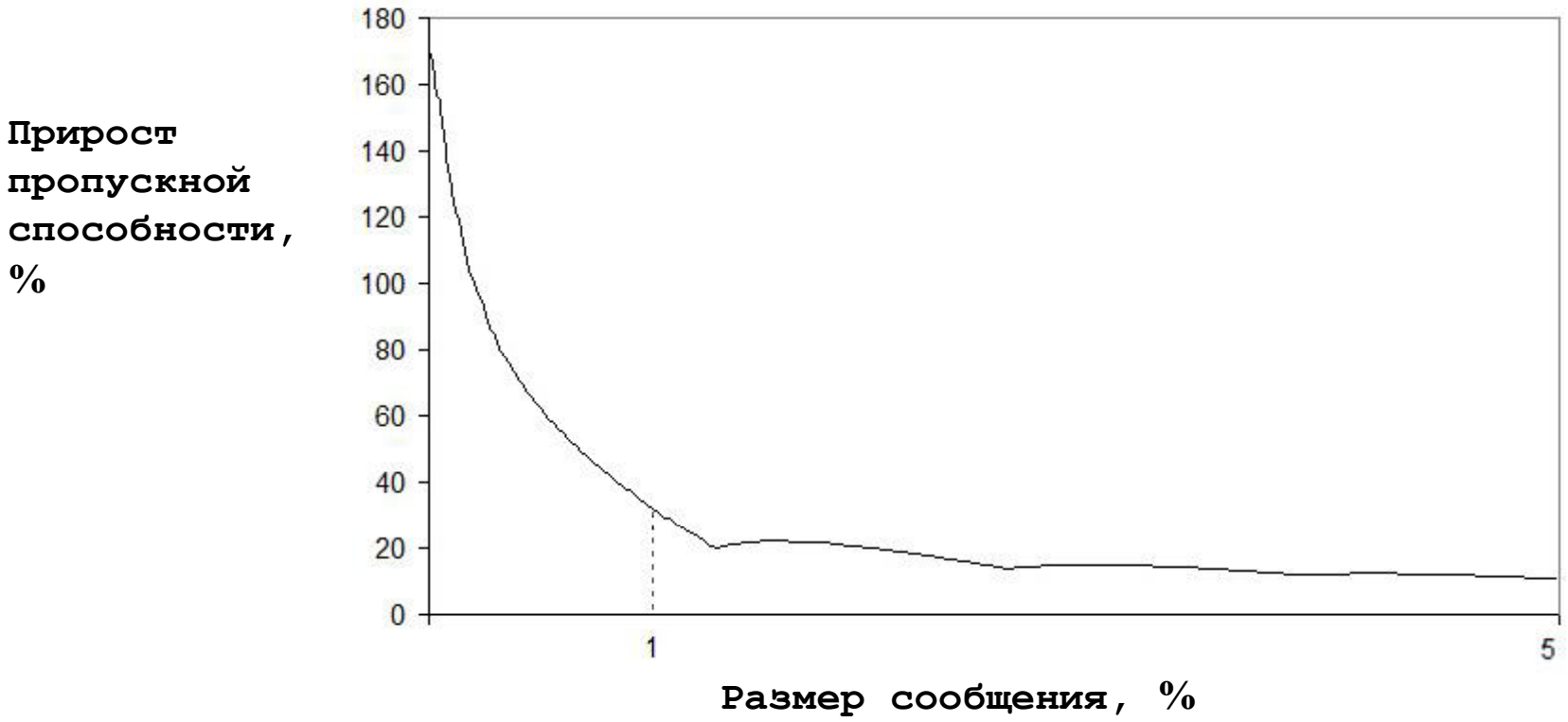
2. Пусть x – решение задачи встраивания *n* бит, а x* - решение аналогичной задачи для *n* + *α* бит, и

$$\frac{\partial D}{\partial x_u} > 0, \frac{\partial^2 D}{\partial x_u^2} > 0, \quad x_u \in \left[0; k_u^*\right], u = \overline{1, m}$$

Тогда

$$x_u^* \geq x_u \quad u = \overline{1, m}$$

Экспериментальные результаты



Зависимость прироста пропускной способности от размера встраиваемого сообщения

Полученные результаты

Использование разработанного метода выбора элементов контейнера позволяет:

- строить абсолютно стойкие к RS-стегоанализу стегосистемы
- увеличить пропускную способность метода LSB, так как в пиксели на границах объектов можно встраивать больший объем информации
- построить JPEG-стегосистему при использовании WP-кодов (wet paper codes, коды «мокрой бумаги»)

Полученные результаты

Использование предложенного подхода позволяет:

- анализировать стойкость стеганографических систем к существующим стегоаналитическим атакам
- оптимизировать скрывающее преобразовании при встраивании информации в цифровые объекты различных форматов
- модифицировать существующие стегоаналитические атаки с учетом полученной информации о более подходящих и менее подходящих для встраивании группах элементов контейнера

Полученные результаты

Использование разработанной модели стегоконтейнера и метода выбора коэффициентов JPEG-изображения для встраивания информации позволяет:

- повысить стойкость стегосистемы при сохранении пропускной способности
- повысить пропускную способность в среднем на 72,2% при встраивании сообщений до 0,01 bpac
- повысить пропускную способность в среднем на 15,7% при встраивании сообщений от 0,01 bpac до 0,05 bpac.
- совмещать оптимизацию скрывающего преобразования с другими методами повышения эффективности встраивания, в частности, с матричным встраиванием

Апробация работы

- **Разделы диссертационной работы были опубликованы в виде тезисов докладов научных конференций:**
  - **Научная школа-семинар с международным участием «Компьютерная безопасность и криптография» SIBECRYPT'10, ТюмГУ, г. Тюмень.**
  - **Научная школа-семинар международным участием «Компьютерная безопасность и криптография» SIBECRYPT'09, ОмГУ, г. Омск.**
  - **IEEE 6th Conference on Cybernetic Systems, 2007, UCD, Dublin.**
  - **«Математика и безопасность информационных технологий» МаВІТ'06, МГУ, Москва.**

Публикации

- **Список опубликованных работ по теме диссертации:**
  - **Разинков Е.В., Латыпов Р.Х. О правиле выбора элементов стеганографического контейнера в скрывающем преобразовании // Прикладная дискретная математика (Приложение), №3, 2010.**
  - **Разинков Е.В., Латыпов Р.Х. Стойкость стеганографических систем // Ученые записки Казанского государственного университета, №2, 2009 (перечень ВАК).**
  - **Разинков Е.В., Латыпов Р.Х. Скрытая передача информации с использованием границ объектов // Ученые записки Казанского государственного университета, №2, 2007 (перечень ВАК)**
  - **Razinkov E.V., Latypov R.Kh. Image Steganograpghy Technique Using Objects Outlines // Proc. of IEEE Conference on Cybernetic Systems, 2007.**
  - **Разинков Е.В., Латыпов Р.Х. Встраивание цифрового водяного знака в изображение с использованием комплексного преобразования Адамара // Тезисы докладов МаВІТ'06, 2006.**

Спасибо за внимание!