Новые алгоритмы стеганографии и стегоанализа, базирующиеся на идеях и методах теории информации

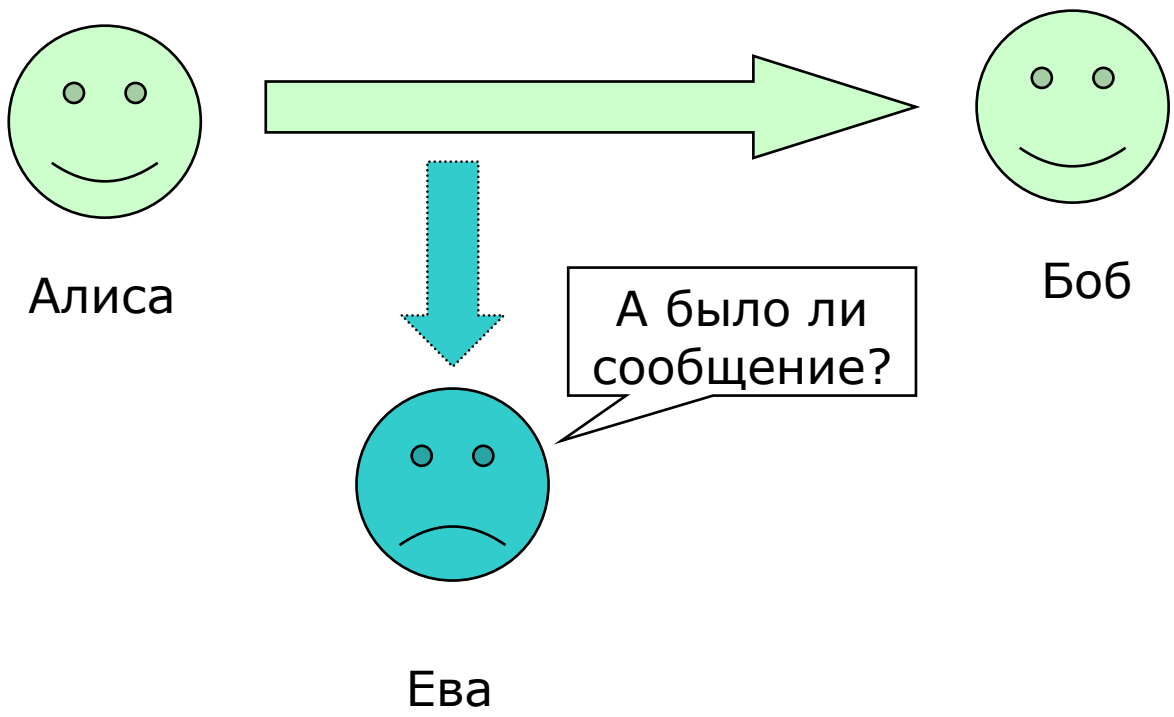
Б. Я. Рябко, А. Н. Фионов

Сибирский государственный университет телекоммуникаций и информатики

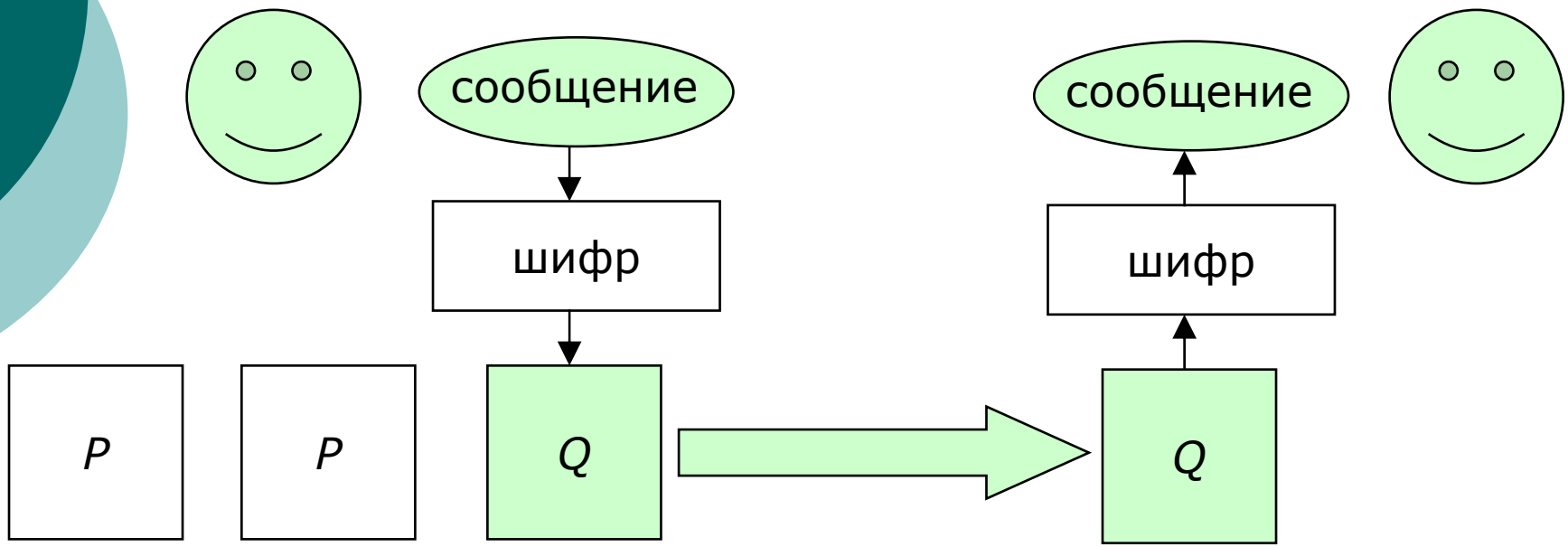
Новосибирск

Задача стеганографии

передать сообщение так, чтобы сам факт передачи остался скрытым



Основная схема



контейнеры

P, *Q* – распределения вероятностей

Алиса посылает Бобу контейнеры. А есть ли в них сообщение?

Два типа стегосистем

- Вычислительно стойкие ($P \approx Q$)
- Совершенные или невскрываемые ($P = Q$)

Идеальные стегосистемы

C. Cachin 1998, 2004

Tri Van Le, K. Kurosawa 2003

P. Moulin, Y. Wang 2004

$P \approx Q$

$P = Q$ только асимптотически

Совершенные стегосистемы

ВПЕРВЫЕ В 2007 г.

предложена конструкция совершенной стегосистемы

$P = Q$

Ryabko B., Ryabko D. Information-theoretic approach to steganographic systems // IEEE International Symposium on Information Theory, Nice, France, 2007. P. 2461—2464.

Основная идея

(на простых примерах)

$X = 0010011110001011$

Контейнер, $p(0) = ?$, $p(1) = ?$

$Y = abba$

Встраиваемое сообщение

$p(a) = p(b)$ т.к. сообщение зашифровано

Обозначим через X^* заполненный контейнер

Основная идея

Символы контейнера группируются по парам.
Пары 00 и 11 остаются без изменения.
Пары 01 и 10 изменяются по правилу a -> 01, b -> 10

00	10	01	11	10	00	10	11	X
	a	b		b		a		Y
	01	10		10		01		
00	01	10	11	10	00	01	11	X^*

Основная идея

00 10 01 11 10 00 10 11 X

a b b a Y

01 10 10 01

00 01 10 11 10 00 01 11 X^*

почему $\Pr(X) = \Pr(X^*)$?

потому, что $\Pr(01)=pq=qp=\Pr(10)$

Основная идея

Переход к блокам из m символов:

кол-во внедряемых бит -> $H(X)$,

где H – энтропия Шеннона

(метод асимптотически оптимален)

Средства реализации

- Быстрая нумерация сочетаний (Рябко 1998)
- Эффективная генерация случайных величин (Фионов 2000)

Другой подход

если известны или могут быть оценены вероятности символов контейнера

Внедряемое сообщение кодируется так, чтобы кодовые символы появлялись с заданными вероятностями.

Другой подход

Омофонное кодирование со стоимостью

(Hoshi, Han 2001; Рябко, Фионов 2007)

Арифметическое декодирование

Работы авторов

- Ryabko B. Fast enumeration of combinatorial objects // Discrete Mathematics and Applications. V. 10, No. 2. 1998.
- Fionov A. Random number generation via homophonic coding // IEEE International Symposium on Information Theory, Sorrento, Italy, June 25–30, 2000. p. 354.
- Ryabko B., Ryabko D. Information-theoretic approach to steganographic systems // IEEE International Symposium on Information Theory, Nice, France, 2007. P. 2461—2464.
- Fionov A., Ryabko B. Simple ideal steganographic system for containers with known statistics // XI International Symposium on Problems of Redundancy. St.-Petersburg, July 2—6, 2007. P. 184—188.

Стеганография в изображениях

LSB-методы

(внедрение информации в наименее значимые биты цветовых составляющих, коэффициентов ДКП и т.д.)

- многочисленные исследования, журналы, конференции
- программы для внедрения (STEGOTOOLS, HIDE4PGP, ...)
- программы для выявления (STEGDETECT, ...)

Стеганография в изображениях

Основные идеи:

- младшие биты заменяются битами внедряемого зашифрованного сообщения
- используется только часть младших бит в соответствии с указанным процентом заполнения

Стеганография в изображениях

Основной недостаток:

- разрываются естественные связи между младшими битами и остальной информацией в изображении
- статистическая структура контейнера изменяется

это даёт возможность обнаруживать скрытые сообщения

Стегоанализ изображений

на основе методов универсального кодирования (сжатия данных)

Пусть X – полученный графический файл
φ – универсальный кодер (архиватор)
Не известно, содержит X скрытые данные или нет

Основная идея:
Копируем X -> Y, внедряем случайные данные в Y -> Y*
Сжимаем X и Y* с помощью φ.
Возможны два случая:
1. $|\varphi(X)| < |\varphi(Y^*)|$ 2. $|\varphi(X)| \approx |\varphi(Y^*)|$

Вопрос: какой случай свидетельствует о наличии в X скрытых данных?

Ответ: 2.

Теоретическое обоснование

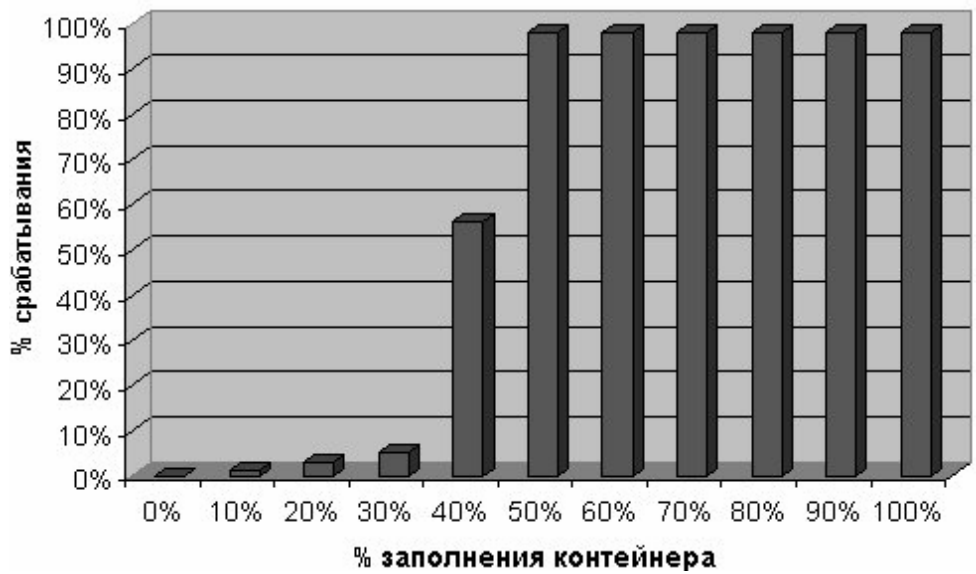
применения универсальных кодов к различным статистическим задачам

- Ryabko B., Astola J. Universal codes as a basis for time series testing // Statistical Methodology. 2006. V. 3. P. 375–397.
- Ryabko B, Astola J. Universal codes as a basis for nonparametric testing of serial independence for time series // Journal of Statistical Planning and Inference. 2006. V. 136, N. 12. P. 4119–4128.

Результаты предлагаемого метода стегоанализа

по программе аспиранта М. Жилкина

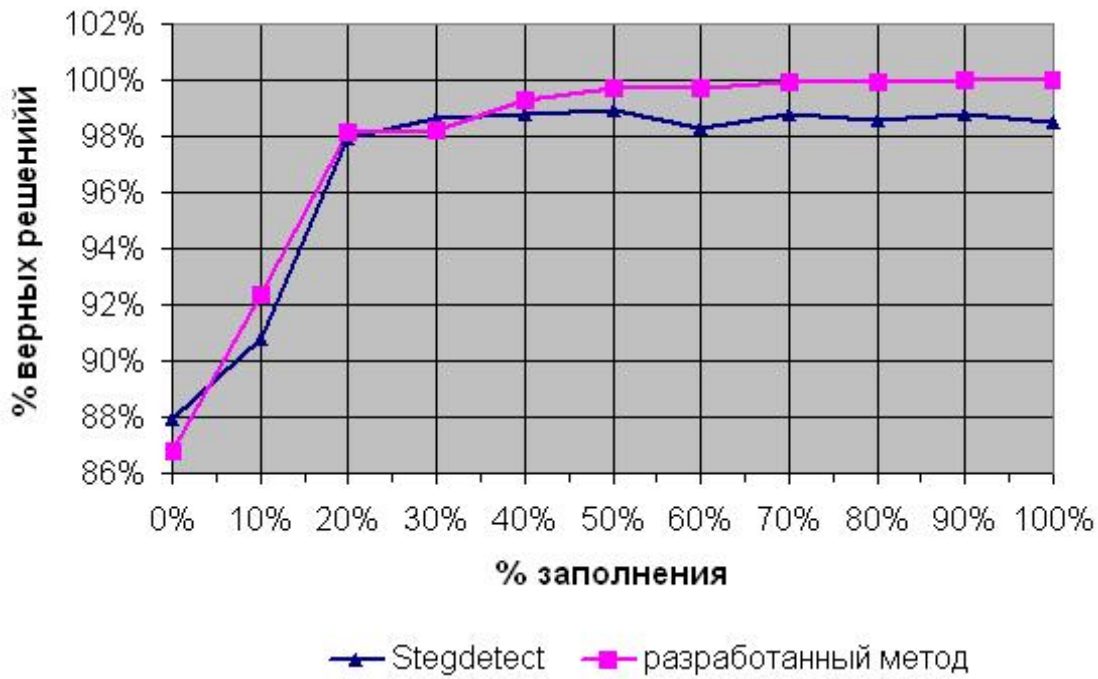
Обнаружение внедрения в BMP-файлы
при различном уровне заполнения



Результаты предлагаемого метода стегоанализа

по программе аспиранта М. Жилкина

Обнаружение внедрения в JPEG-файлы
при различном уровне заполнения



Новый LSB-метод, учитывающий статистику младших бит

Основная идея:

Произвести оценку вероятностей младших бит методами теории универсального (адаптивного) кодирования

Внедрять информацию с учётом статистики младших бит, используя коды со стоимостью (с заданными вероятностями появления кодовых символов)

Отличие от обычного кодирования:

Требуется разделение изображения на обучающую и рабочую области

Новый LSB-метод, учитывающий статистику младших бит

исходное изображение

Новый LSB-метод, учитывающий статистику младших бит

фрагмент левой верней части изображения
в увеличенном масштабе

Новый LSB-метод, учитывающий статистику младших бит

разделение изображения: затенённые пикселы образуют обучающую часть, светлые – рабочую

Новый LSB-метод, учитывающий статистику младших бит

обучающая часть

рабочая часть

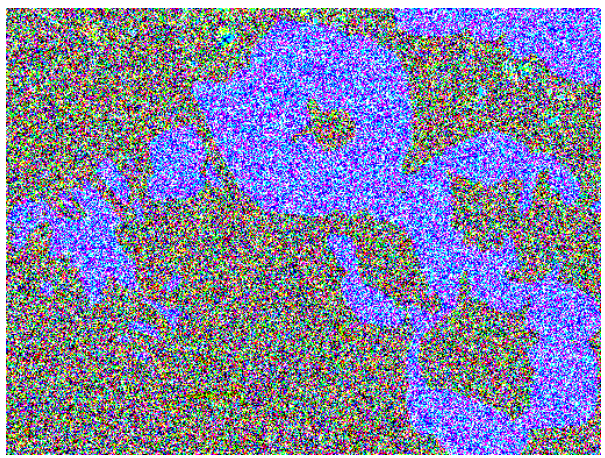
Рабочая гипотеза:

статистические структуры обеих частей близки

Новый LSB-метод, учитывающий статистику младших бит

HIDE4PGP

младшие биты при заполнении на 50%

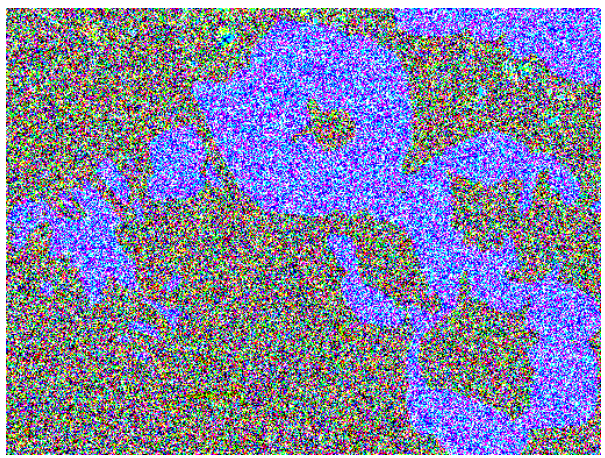


=>

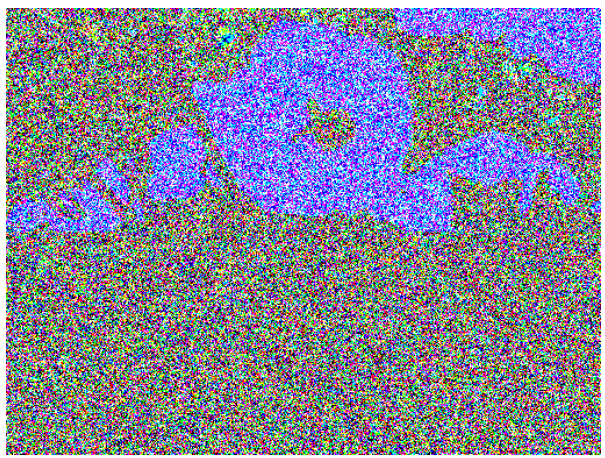
Новый LSB-метод, учитывающий статистику младших бит

STEGOTOOLS

младшие биты при заполнении на 50%



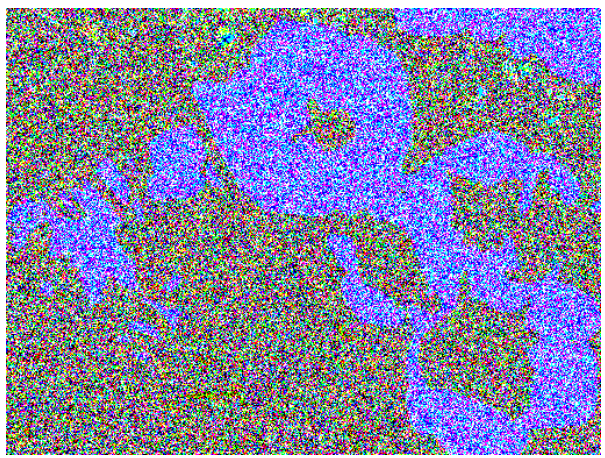
=>



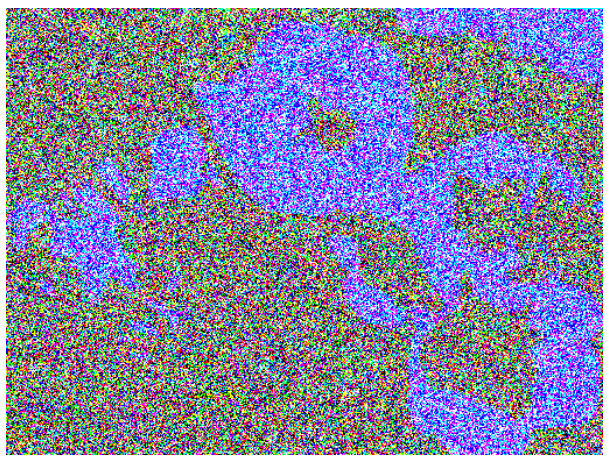
Новый LSB-метод, учитывающий статистику младших бит

Новый метод

младшие биты при заполнении на 50%



=>



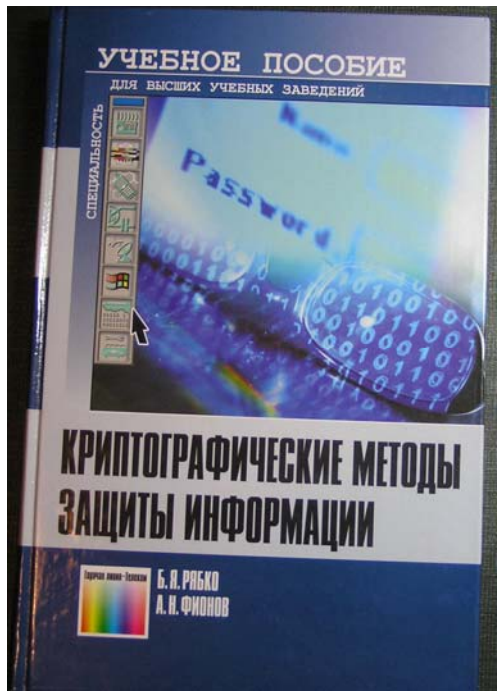
существенно более высокая стойкость к стегоанализу

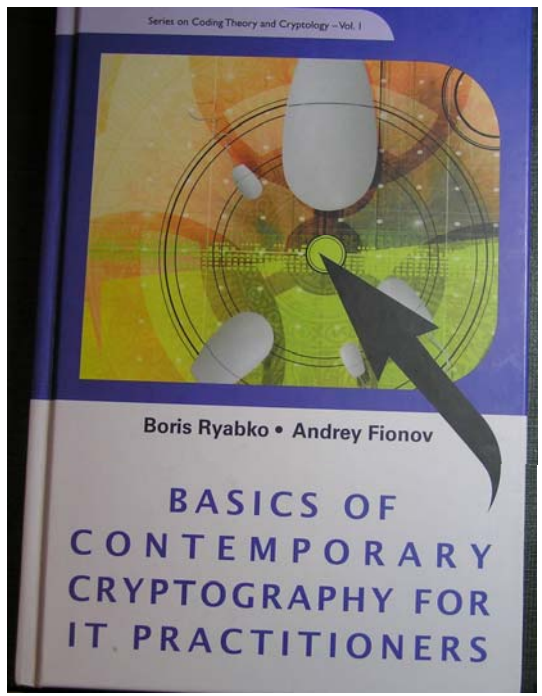
Лаборатория защиты информации

- Рябко Б. Я., д.т.н.
- Фионов А. Н., д.т.н.
- Монарёв В. А., к.ф.-м.н.
- Елтышева Е. Ю., асп.
- Жилкин М. Ю., асп.
- Лубкин А. М., асп.
- Нечта И. В., асп.

Наши книжки


Рябко Б.Я.
Фионов А.Н.
ОСНОВЫ СОВРЕМЕННОЙ КРИПТОГРАФИИ
для специалистов в информационных технологиях
НАУЧНЫЙ МИР


УЧЕБНОЕ ПОСОБИЕ
ДЛЯ ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЙ
СПЕЦИАЛЬНОСТЬ
КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ
Б. Я. РЯБКО
А. Н. ФИОНОВ


Series on Coding Theory and Cryptology – Vol. 1
Boris Ryabko • Andrey Fionov
BASICS OF CONTEMPORARY CRYPTOGRAPHY FOR IT PRACTITIONERS

Благодарю за внимание