Скрытая передача послания посредством шахматной расстановки.

Иванов Вячеслав Евгеньевич

9 класс, Гимназия № 1, Ишимбай, Россия

Научный руководитель: Астафьева Мария Витальевна, учитель информатики, Лицей № 1, г. Салават

Иванов Вячеслав Евгеньевич

Скрытая передача послания посредством шахматной расстановки

АВТОР: ИВАНОВ ВЯЧЕСЛАВ ЕВГЕНЬЕВИЧ, МБОУ ГИМНАЗИЯ №1, Г. ИШИМБАЙ

НАУЧНЫЙ РУКОВОДИТЕЛЬ: АСТАФЬЕВА МАРИЯ ВИТАЛЬЕВНА, МБОУ ЛИЦЕЙ №1, Г. САЛАВАТ, УЧИТЕЛЬ ИНФОРМАТИКИ

Стеганография и криптография

Стеганография - способ передачи или хранения информации с учётом сохранения в тайне факта такой передачи.

Криптография - наука о методах обеспечения конфиденциальности, целостности данных и её аутентификации.

Первые упоминания о применении криптографии появились еще в Древнем Египте в виде иероглифов. Некоторые из них со стороны выглядят как рисунки, но могут обозначать иное.

Документированные способы изготовления стеганографических посланий появились значительно позже. Одним из первых таких способов является царапание по деревянной дощечке и последующее покрытие воском с написанием на нём чего-либо малозначимого.

В отличие от криптографических способов защиты информации, скрывающих содержимое послания, стеганографические способы скрывают сам факт его существования.

Причины выбора темы

- Стремительное развитие информационных технологий
- Компьютеризация многих сфер деятельности
- Рост ценности информации
- Высокий интерес научного сообщества к квантовому компьютеру
- Появление алгоритмов, использующих квантовые явления, которые ставят под угрозу некоторые методы криптографической защиты
- Развитие интереса к некриптографическим средствам защиты информации

Цели исследования

- Понять, каким образом можно скрывать факт передачи сообщения, установить, что может являться контейнером для скрываемого послания, а также каким образом можно одновременно использовать стеганографию и криптографию.
- Определить требования, предъявляемые к стенографической системе
- Создать стеганографическую систему и разработать программный комплекс, решающий задачу как скрытия информации в цифровых объектах, так и приведения послания в изначальное состояние

Характеристика методов сокрытия факта передачи сообщения

- Стегоконтейнер – контейнер, который будет выступать как хранилище для скрываемого сообщения. Им может быть, например, изображение или лист бумаги
- Стегоканал – канал, используемый для передачи послания в стегоконтейнере. Им может выступать, например, запись в интернет-блоге, изображение в профиле пользователя или почтовая служба
- Устойчивость к атакам
- Наличие шифрования с помощью методов криптографии
- Способ шифрования послания – в случае использования методов криптографии

Классификация по устойчивости к атакам на послание

- Хрупкие – разрушающиеся при любом воздействии
- Полухрупкие – устойчивые лишь только к некоторым атакам
- Робастные – устойчивые к любым воздействиям

Направления стеганографии

- Классическая – использование невидимых чернил, проявляющихся под специальным освещением, микроточки – микроскопические фотоснимки, вклеиваемые в письма
- Компьютерная – основанные на особенностях устройства компьютера. Например, скрытие информации в неиспользуемых местах жестких дисков, сохранение информации в зарезервированных полях файлов
- Цифровая – основанные на сокрытии или внедрении дополнительной информации в цифровые объекты. К примеру, замена некоторых битов, отвечающих за яркость или цвет пикселя в изображении

Классические стеганографические способы

Симпатические чернила

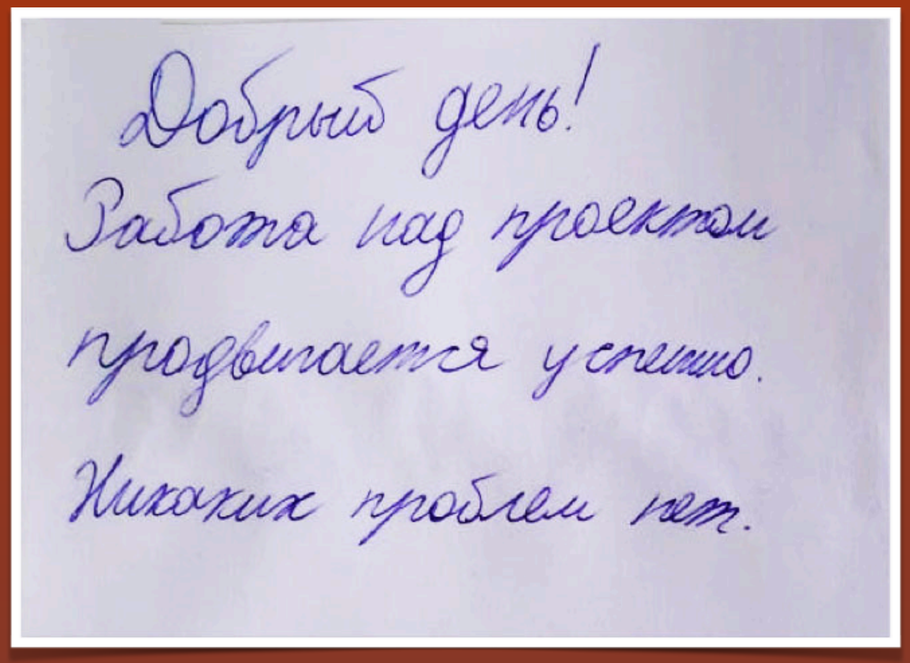
Одним из наиболее распространённых методов классической стеганографии является использование симпатических (невидимых) чернил. Такие методы основаны на химическом взаимодействии чернил и проявителя.

Самые часто используемые чернила и соответствующие им проявители

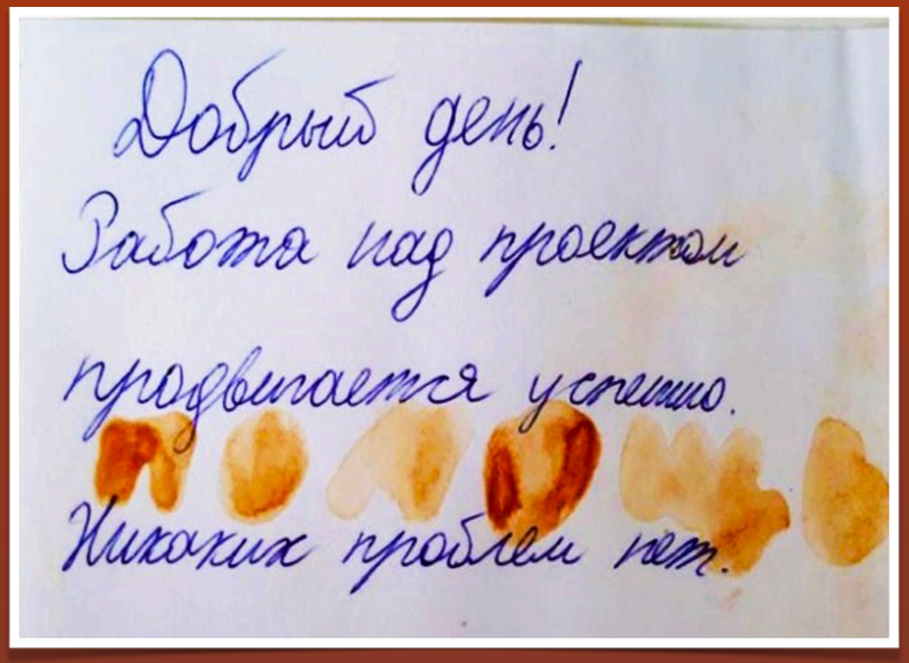
Чернила	Проявитель
Яблочный сок	Нагрев
Молоко	
Сок лука	
Стиральный порошок	Свет ультрафиолетовой лампы
Крахмал	Йодная настойка
Аспирин	Соли железа

Письмо, написанное обычными и симпатическими чернилами

До использования проявителя



После использования проявителя



Преимущества и недостатки использования симпатических чернил

Преимущества:

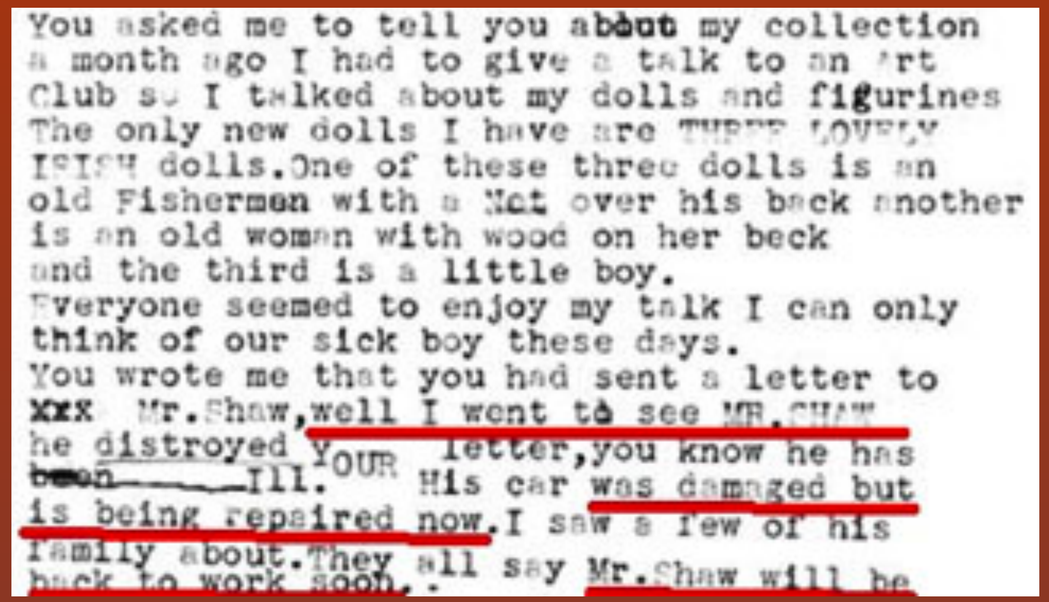
- Простота и скорость изготовления
- Объем послания ограничивается лишь размерами контейнера, в данном случае, бумаги
- Высокая устойчивость к атакам на контейнер

Недостатки:

- Общеизвестность способа
- Контейнер может быть окрашен, приобрести несвойственный ему блеск из-за чернил
- Проблематичность шифрования послания

Специальные шифры

В таких шифрах некоторые слова имеют совершенно иные значения, но употреблены в таком контексте, что со стороны такое послание выглядит как обычное письмо. Ключевое отличие от обычных шифров - единицей послания является не символ, а слово.



You asked me to tell you about my collection
a month ago I had to give a talk to an Art
Club so I talked about my dolls and figurines
The only new dolls I have are THREE LOVELY
IRISH dolls. One of these three dolls is an
old Fisherman with a Net over his back another
is an old woman with wood on her beck
and the third is a little boy.
Everyone seemed to enjoy my talk I can only
think of our sick boy these days.
You wrote me that you had sent a letter to
Xxx Mr. Shaw, well I went to see MR. SHAW
he distroyed YOUR letter, you know he has
been ---- Ill. His car was damaged but
is being repaired now. I saw a few of his
family about. They all say Mr. Shaw will be
back to work soon.

По заявлениям Федерального бюро расследований США, в этом письме, посланном во время Второй мировой войны, под видом обсуждения деталей торговли коллекционными куклами сообщается о завершении починки эсминца и скором его возвращении в состав флота.

Преимущества и недостатки использования специальных шифров

Преимущества:

- Скрытность
- Высокая устойчивость к атакам на контейнер

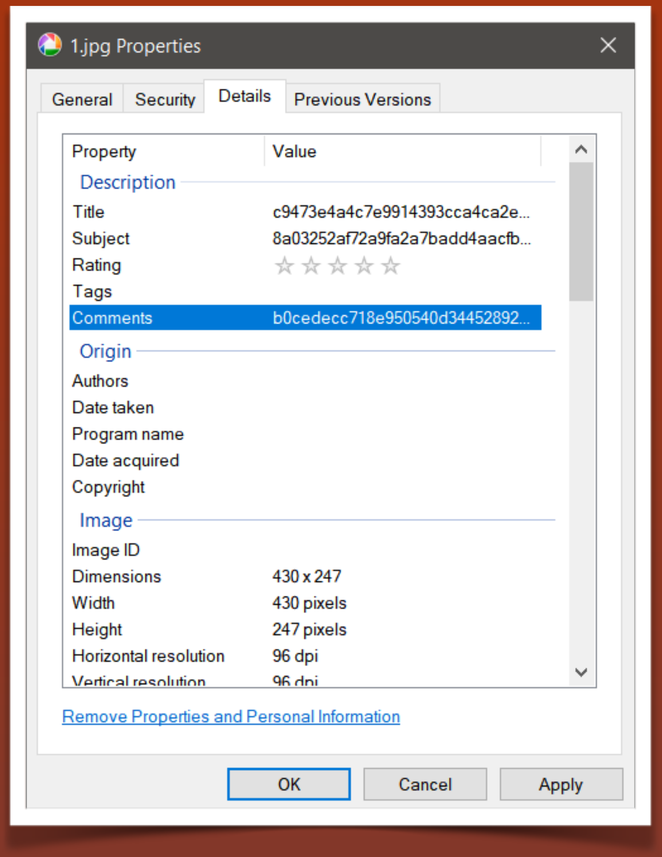
Недостатки:

- Высокая трудоемкость
- Низкий процент содержательной части послания

Компьютерные и цифровые стеганографические методы

Использование особенностей устройства компьютерных систем

Во многих популярных форматах компьютерных файлов имеются используемые зарезервированные поля. Некоторые редко используемые поля по умолчанию заполняются нулями или пустые и могут быть перезаписаны.



Очевидными преимуществами этого метода является его простота и возможность использования криптографии. Но вместе с этим, этот способ имеет низкую степень скрытности.

Во многих файловых системах при хранении на жестком диске файл занимает целое число кластеров. Например, в файловой системе FAT32 стандартный размер кластера – 4 КБ. При хранении 1 КБ информации можно записать ещё 3 КБ информации. Этот способ удобен для хранения маленьких файлов, однако также легко обнаруживается.

Цифровые способы

Гораздо больший интерес представляют способы, использующие в качестве контейнера мультимедийные файлы. Такие данные в большинстве своем имеют большое количество помех и шумов, поэтому, они могут быть использованы для сохранения дополнительной информации, поскольку небольшое изменение картинки, видео или аудио не будет замечено человеческими органами чувств. С их помощью можно передавать большие объёмы информации.

Методы, применимые к изображениям

Метод LSB (Least Significant Bit (наименьший значащий бит)) заключается в встраивании вместо последних значащих битов в контейнере на биты скрываемой информации. Он получил применение в скрытии информации в изображениях, поскольку даже замена двух последних бит незначительно влияет на восприятие изображения в целом.

Пусть имеется изображение, использующее для хранения информации о пикселе 8 бит, и требуется послание длиной 4 бит «1011». Если пиксели имеют вид 00000000 и заменяется только последний бит, то после встраивания сообщения пиксели будут выглядеть так, как продемонстрировано в таблице ниже

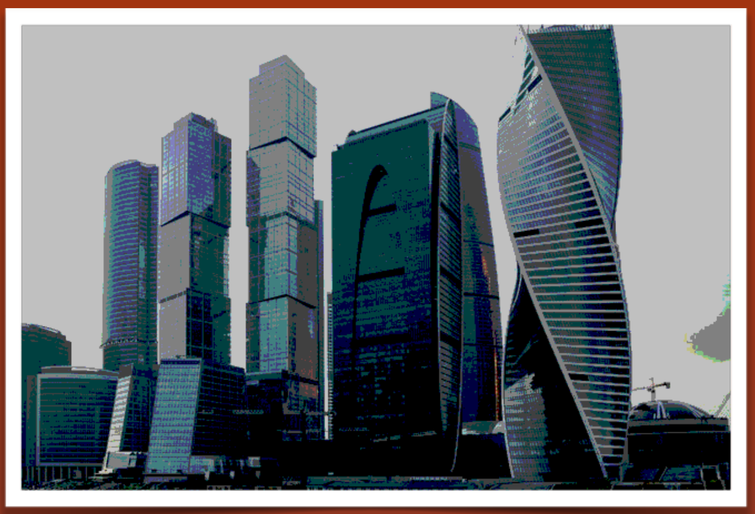
Бит послания	1	0	1	1
Пиксель изображения	0000000<u>1</u>	0000000<u>0</u>	0000000<u>1</u>	0000000<u>1</u>

Пример применения метода LSB

Контейнер для послания

Заполненный контейнер

Извлеченное послание



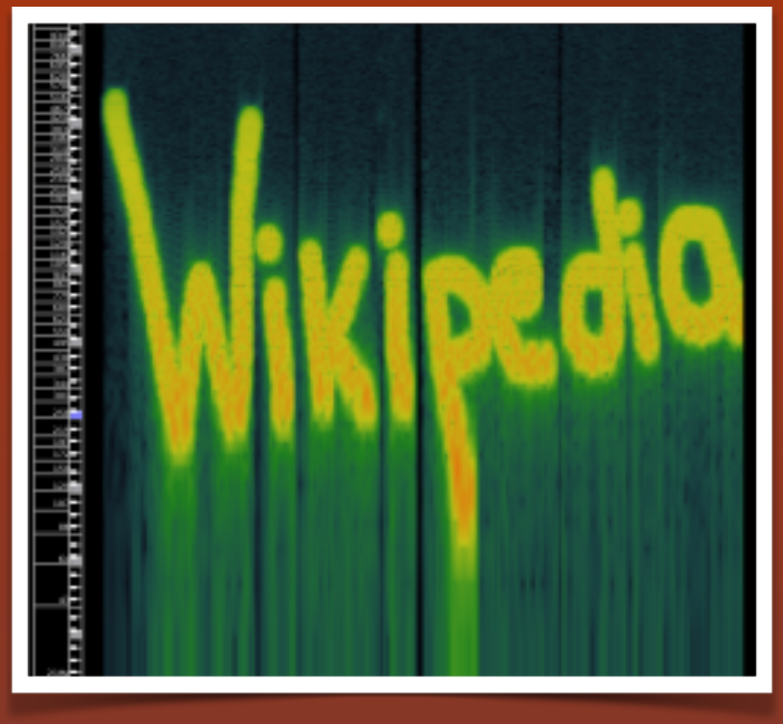
Другой метод, GLM (Grey Level Modification (изменение серого оттенка)), применимый к черно-белым изображениям, похож на предыдущий - четность значения оттенка выражает 1, нечетность – 0.

Оба метода просты, но эффективны. Однако, эти методы, будучи пространственными, то есть манипулирующими пикселями, являются хрупкими, поскольку любое изменение контейнера разрушит целостность послания.

Существуют гораздо более сложные способы, применяющие те же методы, что и сжатие изображений с потерями, которые позволяют сделать сообщение устойчивым к некоторым видам атак на контейнер.

Скрытие послания в звуковой волне

Возможно скрыть послание и в звуке – создать такую последовательность колебаний, которая, при построении спектрограммы, будет выглядеть как текст или другое послание.



Выводы из теоретической части

- Заполненный контейнер должен быть визуально неотличим от пустого
- Стегосистема должна обеспечивать требуемую пропускную способность
- Вычислительная сложность должна быть приемлемой
- Безопасность системы должна дополнительно обеспечиваться методами криптографии – это означает, что даже при знании принципов работы стегосистемы, злоумышленник не сможет установить наличие или отсутствие сообщения в контейнере или извлечь его
- Факт наличия сообщения в данном контейнере не должен влиять на безопасность передачи дальнейших сообщений

Практическая часть

Использование шахматной расстановки как контейнера для стегосистемы

Шахматная игра имеет огромное число исходов. Известный математик Клод Шеннон оценил количество различных шахматных партий в 10^{120}. Можно было бы использовать партии как стегоконтейнер, однако, исходя из критерия приемлемости вычислительной сложности и пропускной способности, такой способ не подходит.

Поэтому, предлагается использовать как контейнер конкретное состояние партии - шахматную расстановку.

Набор из расстановок может передаваться под видом предлагаемых к решению шахматных задач.

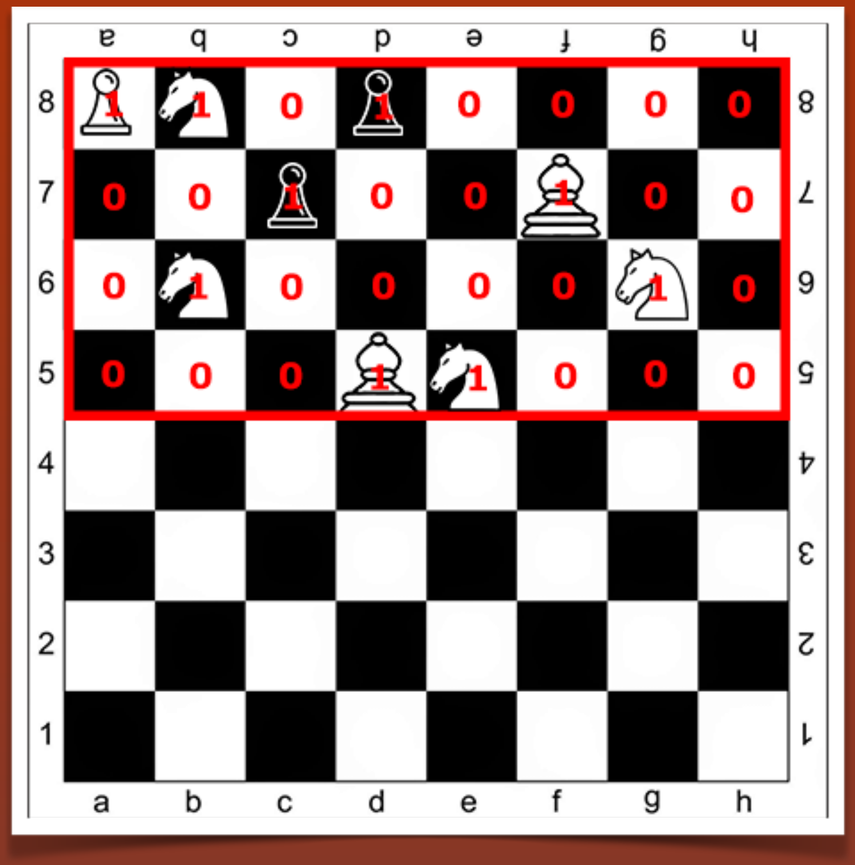
Выбор способа сокрытия послания в состоянии шахматной доски

Согласно выводам, сделанным Клодом Шенноном в своих работах, количество различных шахматных расстановок приблизительно равно 10^{43}. Если принять это количество за мощность некого алфавита, то каждой шахматной расстановкой можно будет передать

$$i = \frac{43 \log 10}{\log 2} = 142 \text{ бит}$$

Что довольно мало, учитывая вычислительную сложность такого метода.

Более реалистичным выглядит метод, использующий наличие или отсутствие фигуры в клетке. Этот способ прост в реализации, но не использует многообразие игровых фигур и применяет лишь половину всех клеток, поскольку имеется всего лишь 32 фигуры.



Выбранный способ

Можно заметить, что ограничениями ранее описанных способов являются постоянность длины послания и пренебрежение использованием разнообразия фигур.

Значит, требуется шифр с динамической длиной послания, а значит и некоторыми метками начала и конца послания. Так можно будет достичь более высокой эффективности способа, то есть отношения объёма «невидимой» информации к объёму контейнера. Возможна ситуация, что послание не получается вместить в одну шахматную расстановку. В таком случае, его следует разбить на послания, которые можно закодировать. Но при задании кодировки следует учитывать то, что каждое разбиение снижает эффективность метода.

Нахождение наилучшего шифра

Назовем гарантированной длиной послания такое неотрицательное целое число n, что при данной кодировке возможно закодировать любое неотрицательное целое число x в диапазоне от 0 до 2^n. Именно от этого значения зависит частота разбиений, а от нее и эффективность метода.

Для однозначности расшифровки метками начала и конца послания выберем фигуры, присутствующие в малом количестве. Пусть это будет ферзь.

Пусть каждая из фигур выражает некоторое количество подряд идущих двоичных единиц, а отсутствие фигуры выражает двоичный ноль.

Для поиска наилучшей последовательности выведем формулу для расчета максимальной и гарантированной длины послания. Будем считать, что наилучший шифр - шифр, имеющий максимальную гарантированную длину послания.

Вывод формул максимальной и гарантированной длин послания

Максимальная длина послания достигается тогда, когда в последовательности сначала подряд идут единицы, а потом нули.

Обозначим фигуры через буквы. Пусть A – пешка, B – король, C - слон, D - ладья, E – конь.

Пусть значением $length(x)$ является длина последовательности из единиц, задаваемая аргументом x.

Тогда максимальная длина последовательности равна сумме произведений количества фигуры x и значения $length(x)$ для данной фигуры. К этому значению нужно прибавить количество всегда свободных клеток на поле, которые будут нулями в конце последовательности.

$$L_{max} = 16 * length(A) + 2 * length(B) + 4 * length(C) + 4 * length(D) + 4 * length(E) + 32$$

Пусть значением $count(x, P)$ является количество последовательностей единиц длины x, которые можно составить из фигур, последовательности которым задает таблица P.

$$L_{guaranteed} = min(count(x, P) * x + x - 1)$$

Для натурального x до некоторого числа.

Эти формулы понадобятся для поиска наилучшей кодировки для стеганографии на шахматной доске.

Наилучшая кодировка

Для поиска наилучшей кодировки была написана программа, перебирающая все возможные кодировки, которая выбирает кодировку с максимальной гарантированной длиной.

Программа «жадным» способом для каждой кодировки считает количество непрерывных последовательностей с разной длиной и выбирает наихудшее значение для каждой кодировки.

При увеличении длины непрерывной последовательности количество единиц в разумных пределах количество единиц, задаваемое каждой фигурой, расположенных в порядке возрастания, стремится к числам Фиббоначи.

Для данной кодировки

$L_{max} = 74$ бит

$L_{guaranteed} = 43$ бит

Шахматная фигура	Последовательность
Пешка	1
Король	1
Слон	1
Ладья	11
Конь	111

Применение полученной кодировки

Несмотря на то, что все этапы передачи информации таким стеганографическим методом могут быть выполнены человеком, было принято решение автоматизировать как процесс создания стего, так и процесс извлечения из него информации, например, для текстового послания.

Для сжатия послания используется особая символьная кодировка в двух версиях: основной и дополнительной. Основная кодировка содержит основные знаки препинания, символы английского алфавита и символы перевода строки и пробела. Каждый символ кодируется 5 битами. В дополнительной кодировке присутствуют еще и буквы русского алфавита и цифры. Каждый символ в ней кодируется 6 битами.

Основная и дополнительная символьные кодировки

A	B	C	D	E	F	G	H	I	J
0	1	2	3	4	5	6	7	8	9
K	L	M	N	O	P	Q	R	S	T
10	11	12	13	14	15	16	17	18	19
U	V	W	X	Y	Z	.	,	!	?
20	21	22	23	24	25	26	27	28	29
Space	New line	0	1	2	3	4	5	6	7
30	31	32	33	34	35	36	37	38	39
8	9								
40	41								

А	Б	В	Г	Д	Е	Ё	Ж	З	И
0	42	1	43	44	4	45	46	47	48
Й	К	Л	М	Н	О	П	Р	С	Т
49	10	50	12	7	14	51	15	2	19
У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь
52	53	23	54	55	56	57	58	59	60
Э	Ю	Я							
61	62	63							

Меры для обеспечения безопасности передачи послания

Для того, чтобы при нарушении последовательности считывания было затруднено обратное извлечение послания, а также для защиты послания, был применен алгоритм криптографии – Шифр Вернама вместе с идеей повторного использования ключа, предложенной автором шифра. Ключ, используемый для симметричного шифрования, при шифровании каждого символа увеличивается на фиксированный шаг, выражающийся простым числом, благодаря чему при потере нескольких частей стеганограммы, расшифровка практически невозможна.

Вместе с использованием необычной кодировки символом, эти меры существенно затрудняют извлечение послания без знания ключа.

Описание алгоритма работы программы

Создание стеганограммы

1. Текст преобразуется в заданную символьную кодировку
2. Числа, полученные из кодировки, преобразуются в последовательность единиц и нулей
3. Коды символов шифруются с помощью симметричного шифра Вернама, увеличивается ключ шифра на константное значение
4. Выбирается расстояние, на котором устанавливается индикатор начала послания
5. Выбирается случайная шахматная фигура и добавляется на доску
6. Устанавливается индикатор окончания послания
7. Добавляются лишние фигуры на доску
8. Если послание не уместилось на одной шахматной доске, алгоритм выполняется для оставшейся части послания с 4 шага

В результате получается одно или несколько изображений с шахматной доской и фигурами на ней

Расшифровка стеганограммы

1. Для каждой клетки на шахматной доске высчитывается её позиция; изображение клетки сравнивается с каждым из образцов шахматных фигур, использованных при создании стеганограммы, путем получения среднеквадратического отклонения гистограммы разницы образца и изображения клетки
2. Проверяется *первое условие цельности стеганограммы (см. далее)*
3. Пропускаются все фигуры, находящиеся вне участка, ограниченного фигурами-индикаторами начала и конца послания
4. Фигурам сопоставляется последовательность единиц и нулей
5. Проверяется *второе условие цельности стеганограммы (см. далее)*
6. Последовательность единиц и нулей расшифровывается с использованием шифра Вернама
7. Последовательность единиц и нулей преобразуется в текст

В результате получается текст, использованный при создании стеганограммы (в случае правильности ключа)

Условия цельности стеганограммы

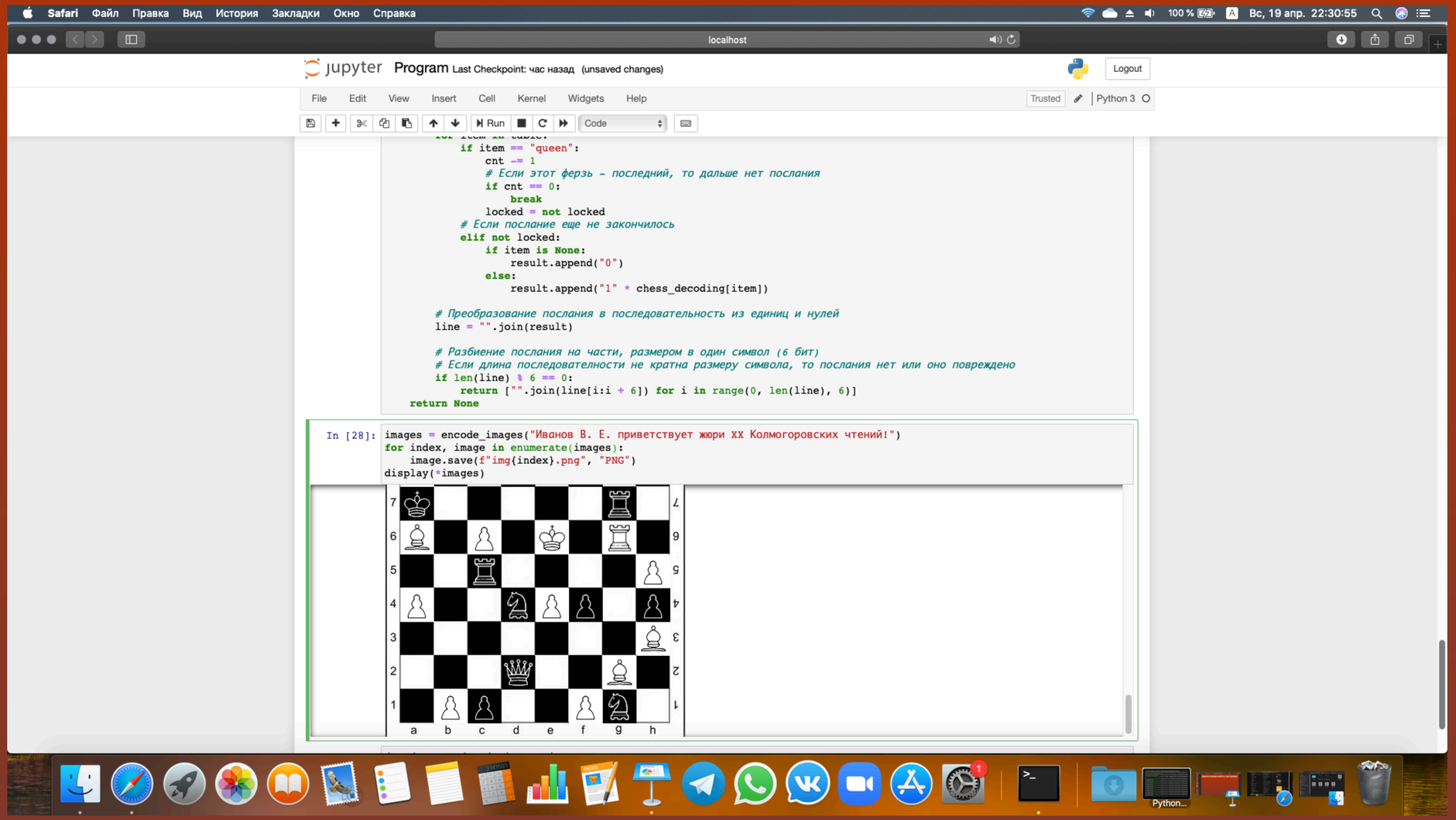
1. Количество фигур-индикаторов начала и конца послания четно, иначе последовательность изображений не является стеганограммой

2. Длина двоичной последовательности кратна длине символа, иначе, последовательность изображений нарушена или не является стеганограммой

Демонстрация работы программы

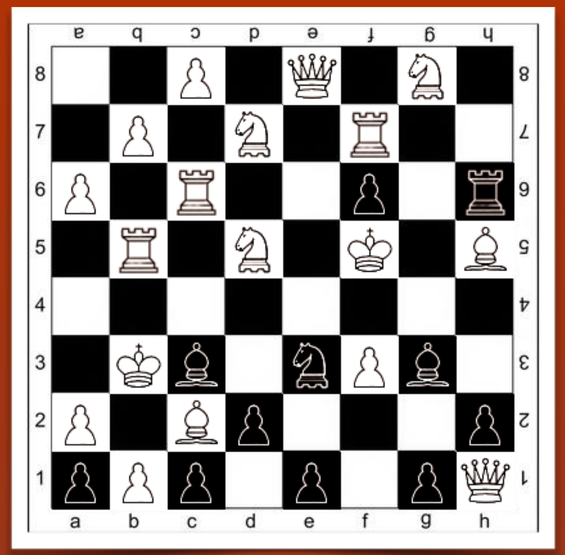
Послание, которое было закодировано в шахматных расстановках

«Иванов В. Е. Приветствует жюри XX Колмогоровских чтений!»

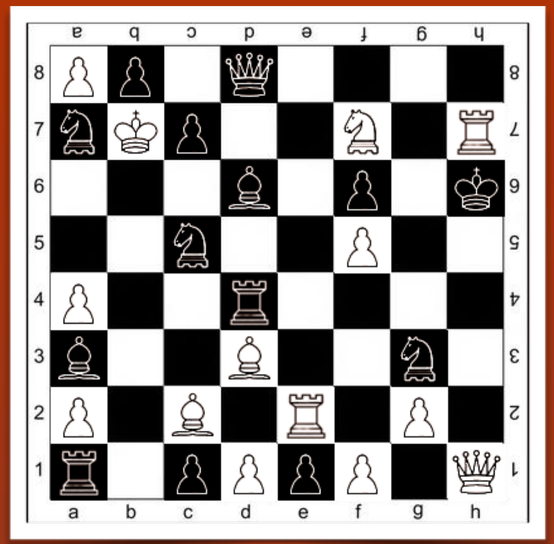


Изображения, созданные программой

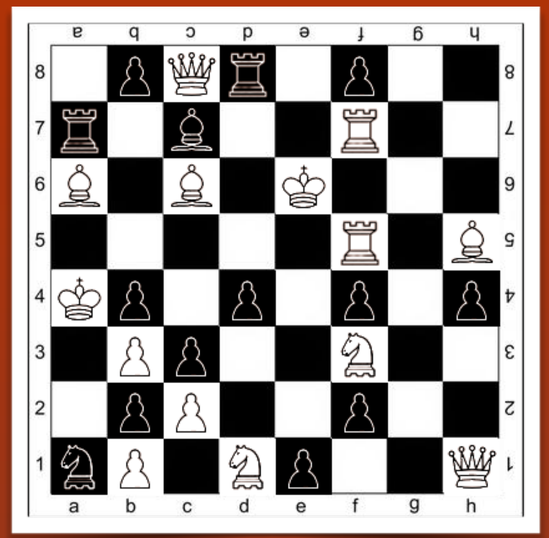
1



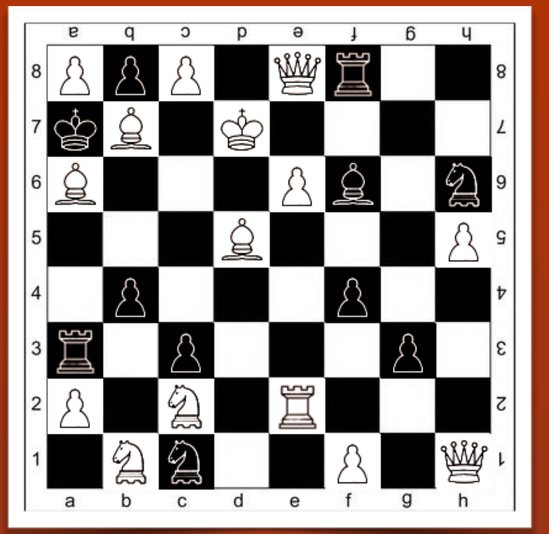
2



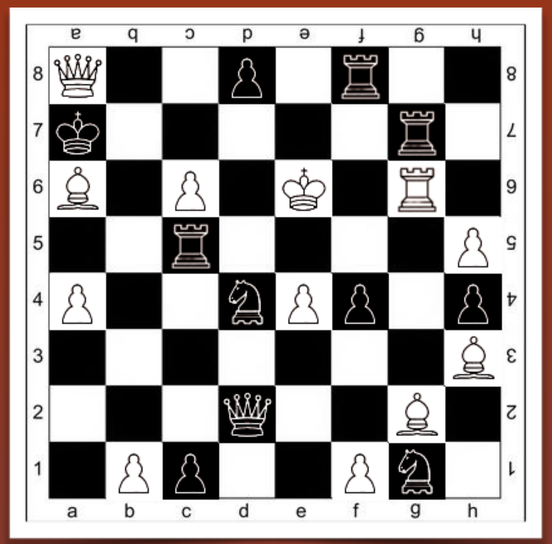
3



4



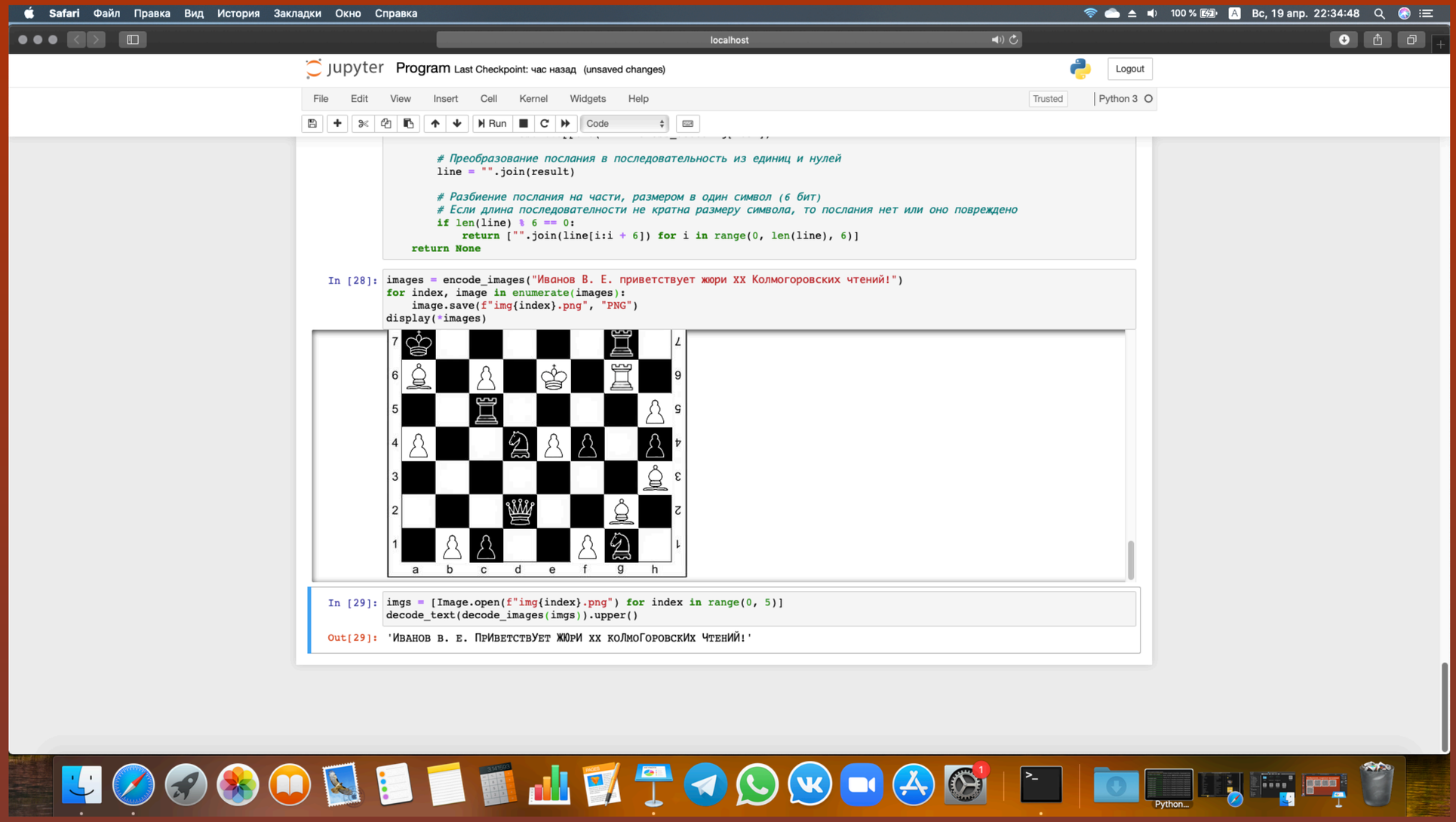
5



Извлечение послания из изображений

Послание, которое вывела программа

«Иванов В. Е. Приветствует жюри XX Колмогоровских чтений!»



Вывод

В результате проделанной работы были установлено, каким образом можно скрыть факт передачи сообщения, установлено что может являться контейнером для скрываемого послания, а также каким образом можно одновременно использовать стеганографию и криптографию.

Были изучены существующие известные стеганографические системы, на основе чего были определены требования, предъявляемые к стеганографической системе.

Был реализован программный комплекс на языке Python с использованием современных библиотек для обработки изображений с учетом определенных ранее требований, позволяющий скрывать информацию в шахматной расстановке и извлекать её обратно, который может быть использован, например, для передачи конфиденциальной информации. На данный момент комплекс использует разнообразие шахматных фигур, но планируется также рассмотреть возможность использования различия в цвете фигуры.

Список использованных источников

1. Бабаш А. В., Гольев, Ю. И., Ларин Д. А. и др. . Криптографические идеи XIX века // Защита информации. Конфидент. — СПб.: 2004. — № 3. [2]

2. Грибунин В. Г., Оков И. Н., Туринцев И. В. Цифровая стеганография. — М. : Солон-Пресс, 2002. — 272 с.

3. P. W. Shor. Algorithms for quantum computation: discrete logarithms and factoring // Proceedings 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, USA. — 1994. — pp. 124-134. [1]

4. Z. Wang, A. C. Bovik. Mean squared error: Love it or leave it? A new look at Signal Fidelity Measures // IEEE Signal Processing Magazine. — 2009. — vol.26 — no. 1 – pp. 98-117 [3]

Спасибо за внимание!