

**Санкт–Петербургский государственный университет**

***Блинов Иван Сергеевич***

**Выпускная квалификационная работа**

***Применение алгоритмов разделения секрета к  
кодированию элементов веб-контента***

Уровень образования: бакалавриат

Направление 01.03.02 «Прикладная математика и информатика»

Основная образовательная программа СВ.5005.2018 «Прикладная математика, фундаментальная информатика и программирование»

Профиль «Исследование и проектирование систем управления  
и обработки сигналов»

Научный руководитель:

профессор, кафедра управления

медико-биологическими системами, д.ф. - м.н.

Утешев Алексей Юрьевич

Рецензент:

профессор, кафедра компьютерного

моделирования и многопроцессорных систем,

д.т.н. Дегтярев Александр Борисович

Санкт-Петербург

2022 г.

# Содержание

|   |           |
|---|-----------|
| <b>Введение . . . . .</b>                                 | <b>3</b>  |
| <b>Цель и постановка задачи . . . . .</b>                 | <b>4</b>  |
| <b>Обзор литературы . . . . .</b>                         | <b>5</b>  |
| <b>Глава 1. Исследование предметной области . . . . .</b> | <b>6</b>  |
| <b>Глава 2. Описание алгоритма . . . . .</b>              | <b>8</b>  |
| <b>Выводы . . . . .</b>                                   | <b>9</b>  |
| <b>Заключение . . . . .</b>                               | <b>10</b> |
| <b>Список литературы . . . . .</b>                        | <b>10</b> |

## Введение

С развитием современных медиа и интернета увеличивается объем передаваемых данных. Вместе с этим растет потребность в безопасности данных, которые представляют собой некоторую ценность. Традиционные методы защиты информации представляет криптография. Чаще всего информация защищается с помощью секретного алгоритма или ключа. Но у такого подхода есть проблемы: если злоумышленник перехватит ключ или скомпрометирует одну из сторон, то он легко получит доступ к секрету.

В 1979 году А. Shamir представил (ссылка) алгоритм разделения секрета, который позволяет разбить секрет на  $n$  долей таким образом, что знание  $K$  и более долей позволяет восстановить секрет, а знание  $K - 1$  и менее долей делает восстановление секрета невозможным. В последние десятилетия было предложено множество алгоритмов разделения секрета для электронных изображений. В данной работе будет рассмотрен и дополнен алгоритм обратимого разделения секрета, реализована библиотека для использования в веб-приложениях и пример минимального проекта, использующего эту библиотеку

## **Цель и постановка задачи**

Целью данной работы является написание библиотеки для языка JavaScript, для разделения секретного цветного электронного изображения, с долями, не подобными шуму. Для достижения этой цели были поставлены следующие задачи:

1. Исследование предметной области
2. Выбор алгоритма
3. Модификация алгоритма для соответствия поставленным требованиям
4. Написание библиотеки
5. Написание минимального веб-приложения, позволяющего продемонстрировать работу программы
6. Тестирование библиотеки и сравнение с имплементациями на других языках

## Обзор литературы

В рамках спецификации современных стандартов, базовые сценарии поведения пользователей призваны к ответу. Банальные, но неопровержимые выводы, а также представители современных социальных резервов формируют глобальную экономическую сеть и при этом - представлены в исключительно положительном свете.

Есть над чем задуматься: предприниматели в сети интернет будут описаны максимально подробно. Приятно, граждане, наблюдать, как сторонники тоталитаризма в науке заблокированы в рамках своих собственных рациональных ограничений. Есть над чем задуматься: некоторые особенности внутренней политики объявлены нарушающими общечеловеческие нормы этики и морали. Как принято считать, тщательные исследования конкурентов смешаны с неуникальными данными до степени совершенной неузнаваемости, из-за чего возрастает их статус бесполезности.

Лишь предприниматели в сети интернет, которые представляют собой яркий пример континентально-европейского типа политической культуры, будут преданы социально-демократической анафеме. Есть над чем задуматься: стремящиеся вытеснить традиционное производство, нанотехнологии являются только методом политического участия и ограничены исключительно образом мышления! Разнообразный и богатый опыт говорит нам, что постоянный количественный рост и сфера нашей активности напрямую зависит от новых предложений.

## Глава 1. Исследование предметной области

Одним из первых алгоритмов разделения секрета является  $(k, n)$  пороговая схема Шамира(ссылка). В ее основе лежит интерполяция полиномов. Пусть  $D$  – некоторая секретная информация, представленная в форме числа. Выберем простое число  $p : p > D, p > N$ . Чтобы разделить секрет на  $n$  частей возьмем случайный полином степени  $k - 1$

$$q(x) = a_0 + a_1x + \dots + a_{k-1}x^{k-1}, a_0 = D, a_i < p$$

и вычислим

$$D_1 = q(1) \bmod p, \dots, D_i = q(i) \bmod p, \dots, D_n = q(n) \bmod p$$

Число  $p$  будет публичным для всех участников, числа  $D_i$  назовем долями.

Имея  $k$  и более долей можно восстановить секрет  $D$  при помощи полиномиальной интерполяции. Допустим злоумышленнику удалось получить доступ к  $k - 1$  долям, тогда для каждого  $D' : 0 < D' < p$  он может восстановить единственный полином степени  $k - 1$ , такой, что  $q_0 = D'$  и  $q_i = D'_i$ . Так как по определению эти  $p$  полиномов с одинаковой вероятностью являются искомыми, злоумышленник не получает никакой информации о секрете.

На основе схемы Шамира были разработаны алгоритмы разделения секрета для изображений. Их можно разделить на три категории - схемы визуальной криптографии(VCS), полиномиальные и схемы, основанные на Китайской теореме об остатках.

В VCS схемах изображение обычно печатается на прозрачных носителях и восстанавливается путем наложения частей друг на друга. Такие схемы обычно характеризуются плохим качеством изображения и значительным увеличением количества пикселей в долях. Их плюсом является отсутствие необходимости вычислений при восстановлении секрета. (ремарка про работу CSS и ссылка )

Полиномиальные схемы используются чаще из-за лучшего качества восстановленного секрета и в общем случае не требуют увеличения количества пикселей. Но у них есть и недостатки - относительно высокая вы-

числительная сложность восстановления секрета  $O(k * \log^2(k))$  и небольшие потери в качестве восстановленного секретного изображения.

В данной работе будет рассматриваться алгоритм за авторством Xuehu Yan, Yuliang Lu, Lintao Liu (ссылка). Он основан на китайской теореме об остатках. В качестве секретной картинке выступает изображение в оттенках серого (0 — 255). Так же вводится понятие изображений для прикрытия — это изображения, использующиеся для генерации долей. Сгенерированные доли являются изображениями в оттенках серого, похожими на изображения прикрытия. Использование изображений прикрытия вместо шумо-подобных долей снижает риск привлечения внимания к долям злоумышленников, улучшает возможности по их менеджменту, позволяет за линейное время восстановить исходную бинарную картинку прикрытия при надобности.

## Глава 2. Описание алгоритма

Начнем описание работы алгоритма с формулировки Китайской теоремы об остатках.

Если  $a_1, \dots, a_n \in N$  попарно взаимно просты, то для

$$\forall r_1, \dots, r_n \in N : 0 \leq r_i < a_i, \forall i \in \overline{1, n}$$

найдется  $N : N \bmod a_i = p_i, \forall i \in \overline{1, n}$

Эта теорема позволяет за линейное время решать систему линейных модулярных уравнений следующего типа:

$$y \equiv a_1 \bmod m_1$$

$$y \equiv a_2 \bmod m_2$$

...

$$y \equiv a_k \bmod m_k$$

Алгоритм решения:

1. Вычисляем  $M = \prod_{i=1}^k m_i$
2.  $\forall i \in \overline{1, k}$  вычисляем  $M_i = \frac{M}{m_i}$
3. С помощью расширенного алгоритма Евклида  $\forall i \in \overline{1, k}$  находим  $M_i^{-1}$  обратное по модулю для  $M_i$
4. Получаем  $y \equiv \sum_{i=1}^k a_i M_i M_i^{-1} \bmod M$

формулировка алгоритма (2-3) стран ремарка про коэф ТН

Описанный алгоритм отлично подходит для цели работы, за исключением цвета картинки. Поэтому было принято решение расширить исходный алгоритм для использования с цветными секретными картинками. Это было достигнуто с помощью увеличения количества пикселей в картинках прикрытия и кодирования каждого канала цвета в определенном пикселе доли.

формулировка улучшения для цветных картинок



более подробный анализ плюсов и минусов полученного алгоритма по сравнению с интерполяционными

рассказ про библиотеку и как я ее офигенно загрузил на npm и какая она в открытом доступе пару слов про приложение со скринами

Нумерованная формула:

$$i^2 = -1. \tag{1}$$

Тест ссылки на формулу 1.

## **Выводы**

Жизнь — тлен.

## **Заключение**

С другой стороны, консультация с широким активом обеспечивает актуальность форм воздействия. Следует отметить, что выбранный нами инновационный путь создает необходимость включения в производственный план целого ряда внеочередных мероприятий с учетом комплекса благоприятных перспектив. В частности, реализация намеченных плановых заданий влечет за собой процесс внедрения и модернизации поэтапного и последовательного развития общества. В частности, новая модель организационной деятельности способствует подготовке и реализации стандартных подходов и тому подобных экспериментов.

## **Список литературы**

- [1] Griffin D.W., Lim J.S. «Multiband excitation vocoder». IEEE ASSP-36 (8), 1988, pp. 1223-1235.
- [2] Griffin D.W., Lim J.S. «Multiband excitation vocoder». IEEE ASSP-36 (8), 1988, pp. 1223-1235.