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

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 A. 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 $k - 1$

$$q(x) = a_0 + a_1 x + ... + a_{k-1} x^{k-1}, a_0 = D, a_i < p$$

и вычислим

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

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 теоремы 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 картинки 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 $a_1, ..., a_n \in N$ попарно взаимно просты, то для

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

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:

$$\begin{aligned} y &\equiv a_1 \bmod m_1 \\ y &\equiv a_2 \bmod m_2 \\ &... \\ y &\equiv a_k \bmod m_k \end{aligned}$$

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 $y \equiv \sum_{i=1}^{k} a_i M_i {M_i}^{-1} \bmod M$

Предложенный алгоритм состоит из двух частей: формирование долей и восстановление секрета. Опишем их более подробно.

2.1 Формирование долей

Описание входных данных:

- Секретное изображение S размера $W_S * H_S$ пикселей в оттенках серого (значения пикселей 0-255)
- n - количество долей
- k - минимальное количество долей для восстановления секрета
- n изображений C_i размера $W_S * H_S$ - бинарные (значения пикселей 0-1) изображения прикрытия для каждого из участников

Описание выходных данных:

- n изображений SC_i размера $W_S * H_S$ - сгенерированные доли
- m_i - приватное число для каждой доли
- p, T - публичные для всех участников числа для восстановления секрета

Алгоритм:

1. Выберем число p и n взаимно простых чисел m_i таких, что

$$128 \leq p < m_i \leq 256, \text{НОД}(m_i, p) = 1, \forall i \in \overline{1, n}$$

2. Вычислим $M = \prod_{i=1}^{k} m_i$, $N = \prod_{i=1}^{k-1} m_{n-i+1}$
3. Если $M < pN$ перейдем к шагу 1
4. Вычислим $T = \left[\frac{\lfloor \frac{M}{p} - 1 \rfloor}{2}\right]$
5. Для каждого секретного пикселя x с координатами $[w, h]$ повторяем шаги 6-7
6. Если $0 \leq x < p$, выберем случайное $A \in [T + 1, \lfloor \frac{M}{p} - 1 \rfloor]$ и вычислим $y = x + Ap$.

   Если $x \geq p$ выберем случайное $A \in [0, T)$ и вычислим $y = x - p + Ap$

7. Если выполняется одно из следующих условий, то вычисляем $a_i = y \bmod p$, устанавливаем $SC_i = a_i$ и переходим к следующему пикселю, иначе возвращаемся на шаг 6.

$$SC_i[w,h] \geq TH_{i1}, \text{ если } C_i[w,h] = 1$$
$$SC_i[w,h] \leq TH_{i0}, \text{ если } C_i[w,h] = 0$$

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 нпм 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.