1 Постановка задачи

Рассматривается задача создания цифровых водяных знаков (digital watermarking) для 2D-векторных данных. Сформулируем ее следующим образом. Есть карта – набор точек плоскости, заданных своими координатами, мы хотим добавить (внедрить) в нее некоторую информацию – наше имя, название компании или что-то еще, что однозначно идентифицирует нас. Естественно, у нас должен быть способ затем извлечь эту информацию из модифицированной карты. В открытый доступ выкладывается только модифицированный нами вариант, таким образом в случае несанкционированного копирования наших данных мы сможем доказать авторство.

Скопировав карту, злоумышленник может ее атаковать – немного изменить, с целью разрушить водяные знаки, не сильно исказив при этом исходные данные. Соответственно, к водяным знакам предъявляется требование – устойчивость против различного рода атак, то есть сохранение возможности извлечения внедренной информации из несильно измененной копии наших данных. Второе естественное требование, предъявляемое алгоритму внедрения, – он не должен сильно искажать исходные данные.

2 Базовый алгоритм

Автором предлагается небольшая модификация алгоритма предложенного Ohbuchi. Изложим его в несколько упрощенном варианте. На входе алгоритма внедрения водяных знаков – множество точек $V = \{v_1, v_2, ..., v_n\}$. Давайте построим триангуляцию Делоне $\mathfrak{T}$ множества V, и рассмотрим граф триангуляции $G(\mathfrak{T})$. Найдем его собственные вектора, как собственные вектора матрицы $R = I - HA$, где $H_{ij} = \begin{cases} 1/deg_i \text{ если } i = j, \\ 0 \text{ иначе;} \end{cases}$ A – матрица смежности графа G. Построим из собственных векторов ортонормированный базис $\mathbb{R}^n$ $\{e_i\}_{i=1}^n$, $n = |V|$. Разложим в этом базисе вектора $x = (x_1, x_2, \ldots, x_n)^T, y = (y_1, y_2, \ldots, y_n)^T$, $(x_i, y_i) = v_i : x = r_1e_1 + r_2e_2 + \ldots r_ne_n, y = s_1e_1 + s_2e_2 + \cdots + s_ne_n$. Если мы хотим внедрить в карту k информационных бит $m_i \in \{-1, 1\}$ $i = 1..k$, то изменим k координат $(r_i, s_i), i = 1..k$ векторов x, y в базисе $\{e_i\}$ на величину $m_ip_i\alpha$, где α некоторый коэффициент, а $\{p_i \in \{-1, 1\}\}$ – псевдослучайная последовательность бит, сгенерированная с помощью некоторого закрытого ключа. Соответственно, выходом алгоритма внедрения будет множества $V' = \{v'_1, v'_2, \ldots, v'_n\}, v_i = (x_i, y_i), x = \sum_{i=1}^n r'_ie_i, y = \sum_{i=1}^n s'_ie_i$;

$$r'_i = r_i + m_ip_i\alpha,\ s'_i = s_i + m_ip_i\alpha. \tag{1}$$

Будем считать, что на вход алгоритма извлечения водяных знаков поступает множество точек $V'' = \{v''_1, v''_2, \ldots, v''_n\}$, причем $|V''| = |V| = |V'|$, и $distance(v'_i, v''_i) < \epsilon$, где ϵ – небольшая погрешность. То есть, мы предполагаем, что злоумышленник только добавил какой-то шум к координатам вершин. Мы вправе предполагать это, так как существуют способы борьбы с другими способами атак или сведения их к небольшим смещениям вершин. При этих предположениях мы извлекаем i-й бит как $m_i = \mathrm{sign}(p_i * (r''_i + s''_i))$, где $r''_i = (e_i, \Delta x), s''_i = (e_i, \Delta y)$ – координаты векторов $\Delta x, \Delta y$ в базисе $\{e_i\}_{i=1}^n$, $(\Delta x_i, \Delta y_i) = (v''_i - v_i)$.

Эксперименты показывают, что предлагаемый Ohbuchi алгоритм имеют хорошую устойчивость против атак, однако не приводится никаких соображений, почему внедряемые водяные знаки не сильно искажают исходные данные, и так ли это в принципе.

3 Оценка искажения

Давайте рассмотрим алгоритм внедрения, как функцию $f : V \to \mathbb{R}^2$, сопоставляющую точкам карты их смещения. Продолжим f на $\Omega = Conv(V)$ – выпуклую оболочку V. Это естественно делать с помощью PLIS (Piecewise Linear Interpolation Surface) по некоторой триангуляции $\mathfrak{T}$ множества V. Действительно, если $f(v_1) = f_1, f(v_2) = f_2, f(v_3) = f_3$, то образом точки $v = \alpha v_1 + \beta v_2 + \gamma v_3, \alpha, \beta, \gamma \in [0, 1], \alpha + \beta + \gamma = 1$ при преобразовании карты логично образом точки v считать точку $v' = v + \alpha f(v_1) + \beta f(v_2) + \gamma f(v_3)$, то есть $f(v) = v - v'$ есть линейная интерполяция f_1, f_2, f_3, если $\triangle T = (v_1, v_2, v_3) \in \mathfrak{T}$. В качестве триангуляции $\mathfrak{T}$ выгодно взять триангуляцию Делоне, так как, согласно теореме Rippa, она минимизирует погрешность PLIS.

В качестве меры искажения исходной карты предлагается взять $E_D(f) = \frac{1}{2}\int_\Omega ||\nabla f||^2 d\Omega$. Эта мера представляется разумной, так как $||\nabla f||$ есть величина, показывающая максимальное изменение f в некоторой точке v, то есть максимум того, насколько v и некоторая близкая к ней точка $v + dv$ “разъезжаются”. Как показал Poithler в случае, когда f есть PLIS множества вершин V по триангуляции $\mathfrak{T}$,

$$E_D(f) = \frac{1}{4}\sum_{\triangle(i,j,k)\in\mathfrak{T}} \operatorname{ctg}\alpha_{ij}||f_i - f_j||^2 + \operatorname{ctg}\alpha_{jk}||f_j - f_k||^2 + \operatorname{ctg}\alpha_{ki}||f_k - f_i||^2,$$

где $f_{\{i,j,k\}} = f(v_{\{i,j,k\}})$, α_{ij} – угол противолежащий ребру (v_i, v_j) в треугольнике $\triangle T = v_i v_j v_k$. Эта формула эквивалентна

$$E_D(f) = \frac{1}{2} \sum_{(i,j)\in E(\mathfrak{T})} w_{ij} ||f_i - f_j||^2,$$

где $E(\mathfrak{T})$ – множество ребер триангуляции, $w_{ij} = \frac{1}{2}(\operatorname{ctg}\alpha_{ij} + \operatorname{ctg}\alpha_{ji})$, $\alpha_{\{ij,ji\}}$ – углы противолежащие ребру (v_i, v_j) в соседних треугольниках $\triangle T_1 = v_i v_j v_{k_1}, \triangle T_2 = v_j v_i v_{k_2}$. Пусть G – взвешенный граф триангуляции $\mathfrak{T}$, $V(G) = V, E(G) = E(\mathfrak{T}$, $weight(u,v) = w_u v$. Если рассмотреть лапласиан L графа G – матрицу $n \times n$, где $n = |V(G)|$, $L_{uv} = \begin{cases} \sum_{(v,x)\in E(G)} w_{vx} \text{ при} & u = v; \\ -w_{uv} \text{ при} & u \sim v; \\ 0 & \text{иначе;} \end{cases}$ то последнюю формулу можно переписать в виде

$$E_D(f) = \frac{1}{2} f^T L f,$$

где $f = (f_1, f_2, \dots f_n)^T$. Откуда видно, что, для $f = \alpha \sum_{i=1}^{k} p_i e_i$, где α – некоторое число, $p_i \in \{-1, 1\}$, $\{e_i\}_{i=1}^{k}$ – набор ортонормированных векторов в $\mathbb{R}^n$, минимум энергии $E_D(f)$ достигается при e_i равных собственным векторам L соответствующим k наименьшим собственным числам.

4 Выводы

Если модифицировать алгоритм Ohbuchi внедрения водяных знаков, так чтобы для изменения по формуле **??** выбиралось k наименьших координат векторов x, y в базисе собственных векторов взвешенного графа триангуляции Делоне, то минимизируется искажения исходных данных в смысле предложенной меры $E_D(f) = \frac{1}{2}\int_\Omega ||\nabla f||^2 d\Omega$.