Algorithm

张昌硕、代金祥

2021 年 2 月 22 日

1 数字签名

使用 $MD5$ 摘要算法进行数字签名，如:

$$MD5(abcdef) = e80b5017098950fc58aad83c8c14978e$$

2 预处理

2.1 签名预处理

将签名字符串转换为二维十进制 list(签名必须长度是 2 的倍数)，如将 $MD5(abcdef) = e80b5017098950fc58aad83c8c14978e$ 转换为：

$$\begin{bmatrix} [14,8,0,11,5,0,1,7,0,9,8,9,5,0,15,12] \\ [5,8,10,10,13,8,3,12,8,12,1,4,9,7,8,14] \end{bmatrix} \tag{1}$$

2.2 编码分区

将字符 ch 分区到

$$i = unicode(ch)\%n$$

其中 n 为 list 的列数，此时对 ch 的 x 轴改变量为 $ls[0][i]$，y 轴改变量为 $ls[1][i]$。

3 放入信息

SVG 是一种基于 XML 语法的图像格式，记录内容为对图像的形状描述。$Fontforge.export()$ 导出的 svg 图片的字形信息均在 xml 的基本形状的 $<path>$ 元素中，其中 d 属性只包括 $\{M, h, v, l, q, t, z\}$ 命令。具体请看此链接：svg 中 path 标签的用法。

由于 $Fontforge$ 记录字形信息只能是整数，所以我们的改变就必须限定为整数改变，否则很难提取出准确的信息。

3.1 q 命令添加信息

q 命令为绘制二阶贝塞尔曲线，由于终点位置不能改变我们将信息加入到控制点的信息中，并考虑到改动幅度应与曲线长度基本成正比，具体变化为：

$$\begin{cases} ctrl_x = ctrl_x + list[0][i] * (dx//\alpha) \\ ctrl_y += ctrl_y + list[1][i] * (dy//\alpha) \end{cases} \tag{2}$$

其中 α 为自定义参数（可改变以得到想要的字体），dx, dy 为 q 命令的第三、四个参数，i 为编码分区。

3.2 h 命令添加信息

$(h \quad dx)$ 变化为 q 命令 $(q \quad dx//2 \quad ctrl_y \quad dx \quad 0)$：

$$ctrl_y = list[1][i] * (dx//\beta) \tag{3}$$

其中 β 为自定义参数（同 α）。

3.3 v 命令添加信息

$(v \quad dy)$ 变化为 q 命令 $(q \quad ctrl_x \quad dy//2 \quad 0 \quad dy)$：

$$ctrl_x = list[0][i] * (dy//\beta) \tag{4}$$

3.4 l 命令添加信息

$(l \quad dx \quad dy)$ 变化为 q 命令 $(q \quad ctrl_x \quad ctrl_y \quad dx \quad dy)$：

$$\begin{aligned} ctrl_x &= dx//2 + list[0][i] * (dx//\beta) \\ ctrl_y &= dx//2 + list[1][i] * (dy//\beta) \end{aligned} \tag{5}$$

4 提取信息

放入信息逆变换可得原信息，该过程要在服务端进行，因为需要转变前的字库与改变后的字库进行比对，客户端可能没有原字库。