07.5 通用隐写分析

钮心忻、杨榆、雷敏 北京邮电大学信息安全中心 yangyu@bupt.edu.cn

通用隐写分析

- 0 原理
 - 通用隐写分析与专用隐写分析
 - 通用隐写分析框架
 - 主要通用隐写分析模型
- 0 空域富模型

通用隐写分析原理

专用隐写分析

早期隐写分析研究方法,思路大体为寻找隐写过程中修改的统计特征,并基于此设计检测算法。特点是"专用",一个隐写分析算法仅对一个隐写算法有效。例如,卡方分析。

通用隐写分析

- 专用隐写分析方法显然难以适应隐写算法快速发展的特点,研究者希望能寻找到对所有或多数隐写算法都有效的分析算法。这一目标过于理想,难以达成。
- 现有阶段,通用隐写分析实际指分析方法通用,更具体的说, 是隐写特征通用。例如,SRM特征几乎能检测同期所有隐写 算法。

通用隐写分析原理

通用隐写分析框架

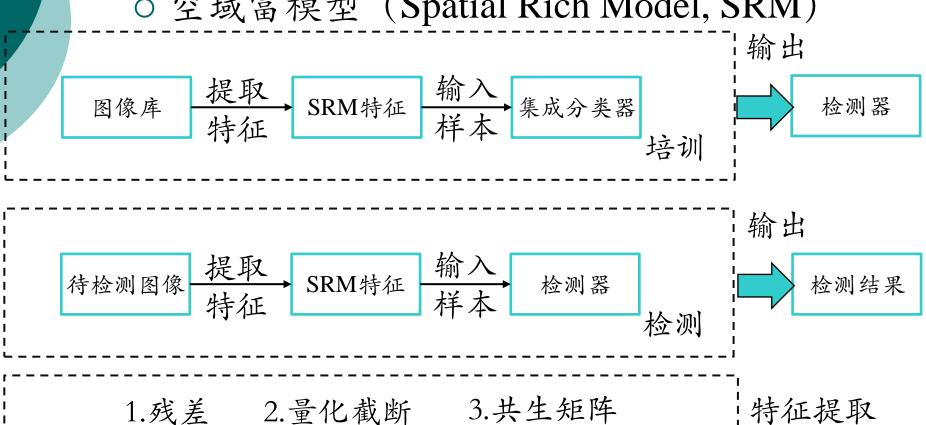
现有通用隐写分析蜕化为通用特征。

通常选定一个特征模型和机器学习算法,结合特定隐写算法培训产生检测器。

○ 主要通用隐写分析模型

- SPAM: SRM模型的前身
- SRM:在SPAM基础上,丰富了滤波器,捕捉了多个方向上的像素相关性的变化。
- maxSRMd2: SRM变种,强调了自适应特性。
- PSRM: SRM变种,降低了计算量,更充分地捕捉了隐写痕迹。
- JRM: SRM的JPEG隐写算法检测版。

○ 空域富模型 (Spatial Rich Model, SRM)

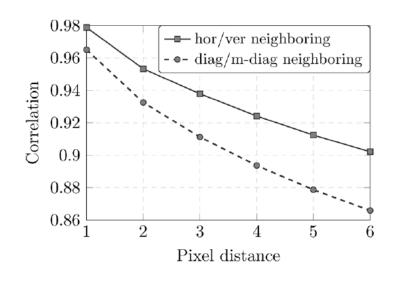


3. 共生矩阵

残差

图像内容与隐写算法无关, 因此,直接根据图像内容提 取特征显然是不明智的。

- 研究显示,图像相邻像素之间具有较强的相关性,而隐写会破坏这种相关性。这一痕迹可通过残差检测。
- 残差定义为像素预测值与像 素值之差。



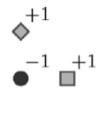
空域富模型—残差计算

SRM定义了丰富的残差以充分捕获相关性的变化。分为 1st和3rd, 2nd, SQUARE, EDGE3x3, 和 EDGE5x5这5个类

水平方向。 别。 $R_{ij} = X_{i,i+1} - X_{ii}$ (一)阶)。 1阶和3阶有 垂直方向。 1a) spam14h,v 8个模板 $R_{ij} = X_{i-1,i} - X_{ii} \ (-\beta)$ $R_{ij} = -X_{i-2,j} + 3X_{i-1,j} - 3X_{ij} + X_{i,j-1} \ (\exists)$ 水平。 $R_{ij} = min\{X_{i,j+1} - X_{i,j}, X_{i,j-1} - X_{i,j}\}$ (— β) $+1 \quad -1 \quad +1 \quad R_{ij} = min \begin{cases} -X_{i,j+2} + 3X_{i,j+1} - 3X_{ij} + X_{i,j-1}, \\ -X_{i,j-2} + 3X_{i,j-1} - 3X_{ij} + X_{i,j+1} \end{cases} (\equiv)$ 垂首。 1b) $\min\max 22h, v \mid R_{ij} = \min\{X_{i-1,j} - X_{ij}, X_{i+1,j} - X_{ij}\}$ (一阶) $R_{ij} = min \begin{cases} -X_{i-2,j} + 3X_{i-1,j} - 3X_{ij} + X_{i+1,j}, \\ -X_{i+2,j} + 3X_{i+1,j} - 3X_{ij} + X_{i-1,j} \end{cases} (\equiv)$

2024/11/24

1阶和3阶滤波器



1c) minmax24

$$R_{ij} = min\{X_{i-1,j} - X_{ij}, X_{i,j+1} - X_{ij}\} \quad (-)$$

$$R_{ij} = min\{-X_{i-2,j} + 3X_{i-1,j} - 3X_{ij} + X_{i+1,j}, -X_{ij}\} \quad (\equiv)$$

│ 水平 ↓

1d) minmax34h,v

$$R_{ij} = min \begin{cases} -X_{i,j+2} + 3X_{i,j+1} - 3X_{ij} + X_{i,j-1}, \\ -X_{i,j-2} + 3X_{i,j-1} - 3X_{ij} + X_{i,j+1}, \\ -X_{i-2,j} + 3X_{i-1,j} - 3X_{ij} + X_{i+1,j} \end{cases} \ (\underline{\equiv} | \widehat{\beta} \widehat{\beta}) \quad (\underline{\equiv} | \widehat{\beta} \widehat{\beta}) \quad (\underline{\equiv} | \widehat{\beta} \widehat{\beta} \widehat{\beta})$$

$$R_{ij} = \min\{X_{i-1,j} - X_{ij}, X_{i,j+1} - X_{ij}, X_{i,j-1} - X_{ij}\} \ (-\beta)$$

垂直。

水平↵

$$R_{ij} = min \begin{cases} -X_{i-2,j} + 3X_{i-1,j} - 3X_{ij} + X_{i+1,j}, \\ -X_{i,j-2} + 3X_{i,j-1} - 3X_{ij} + X_{i,j+1}, \\ -X_{i-2,j} + 3X_{i-1,j} - 3X_{ij} + X_{i+1,j} \end{cases} (\exists \beta)$$

 $R_{ij} = \min\{X_{i-1,j} - X_{ij}, X_{i-1,j} - X_{ij}, X_{i,j-1} - X_{ij}\} \quad (-\beta)$

残差(1阶和3阶)

$$R_{ij} = min\{X_{i-1,j} - X_{ij}, X_{i,j+1} - X_{ij}, X_{i,j-1} - X_{ij}, X_{i+1,j} - X_{ij}\} \quad (-\text{M})$$

$$R_{ij} = min\{X_{i-1,j} - X_{ij}, X_{i,j+1} - 3X_{ij} + X_{i,j-1}, -X_{ij}\} \quad (\text{M})$$

$$-X_{i,j-2} + 3X_{i,j-1} - 3X_{ij} + X_{i,j+1}, -X_{ij}\} \quad (\text{M})$$

$$-X_{i-2,j} + 3X_{i-1,j} - 3X_{ij} + X_{i+1,j}, -X_{i+1,j}\} \quad (\text{M})$$

$$1\text{M} \approx 3\text{M} \approx 3$$

$$\stackrel{+1}{\diamond}\stackrel{+1}{\vartriangle}^{+1}$$

$$R_{ij} = min\{X_{i-1,j} - X_{ij}, X_{i,j+1} - X_{ij}, X_{i-1,j+1} - X_{ij}\} \quad (-|\hat{y}|)$$

$$R_{ij} = min\{ -X_{i-2,j} + 3X_{i-1,j} - 3X_{ij} + X_{i+1,j}, -X_{i,j+2} + 3X_{i,j+1} - 3X_{ij} + X_{i,j-1}, -X_{i-2,j+2} + 3X_{i-1,j+1} - 3X_{ij} + X_{i+1,j-1} \} \quad (\equiv |\hat{y}|)$$

残差(1 除和3 除) _{Rii}:

水平。
$$R_{ij} = min\{X_{i-1,j} - X_{ij}, X_{i,j+1} - X_{ij}, X_{i-1,j+1} - X_{ij}, X_{i-1,j-1} - X_{ij}\} \quad (-)$$
) ()

$$R_{ij} = min \begin{cases} -X_{i-2,j} + 3X_{i-1,j} - 3X_{ij} + X_{i+1,j}, \\ -X_{i,j+2} + 3X_{i,j+1} - 3X_{ij} + X_{i,j-1}, \\ -X_{i-2,j+2} + 3X_{i-1,j+1} - 3X_{ij} + X_{i+1,j-1}, \\ -X_{i-2,j-2} + 3X_{i-1,j-1} - 3X_{ij} + X_{i+1,j+1} \end{cases}$$
 ($\equiv \mathbb{N}$)

垂直。

水平。

□ ⁺¹ ♦ ⁺¹ Δ ⁺¹	实三 ↩	<u>实方</u> ↩	φ
	<u>实菱</u> ↩	黑点~	φ
● ■ +1	空方↩	÷.	e.

1阶和3阶滤波器

1g) minmax48h,v

$$R_{ij} = \min\{X_{i-1,j} - X_{ij}, X_{i,j-1} - X_{ij}, X_{i+1,j-1} - X_{ij}, X_{i-1,j-1} - X_{ij}\} \quad (-1)$$

$$R_{ij} = min \begin{cases} -X_{i-2,j} + 3X_{i-1,j} - 3X_{ij} + X_{i+1,j}, \\ -X_{i,j-2} + 3X_{i,j-1} - 3X_{ij} + X_{i,j+1}, \\ -X_{i+2,j-2} + 3X_{i+1,j-1} - 3X_{ij} + X_{i-1,j+1}, \\ -X_{i-2,j-2} + 3X_{i-1,j-1} - 3X_{ij} + X_{i+1,j+1} \end{cases}$$
 ($\equiv \mathbb{R}$)

残差(1阶和3阶)

 $\square^{+1} \diamondsuit^{+1} \triangle^{+1}$ $-1 \square^{+1}$ \triangle^{-1}

1g) minmax54

1阶和3阶滤波器

$$R_{ij} = min \begin{cases} X_{i-1,j} - X_{ij}, \\ X_{i,j+1} - X_{ij}, \\ X_{i-1,j+1} - X_{ij}, \\ X_{i-1,j-1} - X_{ij}, \\ X_{i+1,j+1} - X_{ij} \end{cases} \quad (-\beta)$$

$$R_{ij} = min \begin{cases} -X_{i-2,j} + 3X_{i-1,j} - 3X_{ij} + X_{i+1,j}, \\ -X_{i,j+2} + 3X_{i,j+1} - 3X_{ij} + X_{i,j-1}, \\ -X_{i-2,j+2} + 3X_{i-1,j+1} - 3X_{ij} + X_{i+1,j-1}, \\ -X_{i-2,j-2} + 3X_{i-1,j-1} - 3X_{ij} + X_{i+1,j+1}, \\ -X_{i+2,j+2} + 3X_{i+1,j+1} - 3X_{ij} + X_{i-1,j-1} \end{cases} \quad (\exists \beta)$$

每个 min 都有一个对应的 max -

空域富模型—残差计算

残差(2阶)

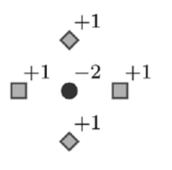
2阶滤波器

$$\blacksquare^{+1} \bullet^{-2} \blacksquare^{+1}$$

水平。
$$R_{ij} = X_{i,j+1} + X_{i,j-1} - 2X_{ij} \quad (三阶)$$
垂直。
$$R_{ij} = X_{i,j+1} + X_{i,j-1} - 2X_{ij} \quad (三阶)$$

$$R_{ij} = X_{i-1,j} + X_{i+1,j} - 2X_{ij} \ (\Box)$$

2a) spam12h,v



2024/11/24

$$R_{ij} = min \begin{cases} X_{i-1,j} + X_{i+1,j} - 2X_{ij}, \\ X_{i,j+1} + X_{i,j-1} - 2X_{ij} \end{cases} \; (\square) \quad \text{.}$$

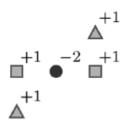
信息隐藏与数字水印

空域富模型一残差计算

残差(2阶)

2阶滤波器

$$R_{ij} = min \begin{cases} X_{i-1,j} + X_{i+1,j} - 2X_{ij}, \\ X_{i,j+1} + X_{i,j-1} - 2X_{ij}, \\ X_{i-1,j+1} + X_{i+1,j-1} - 2X_{ij}, \\ X_{i-1,j-1} + X_{i+1,j+1} - 2X_{ij}, \end{cases}$$
(\square S)



2d) minmax24h,v

$$R_{ij} = min \begin{cases} X_{i-1,j} + X_{i+1,j} - 2X_{ij}, \\ X_{i-1,j-1} + X_{i+1,j+1} - 2X_{ij} \end{cases} (\square \%)$$

2024/11/24

残差(2阶)

2阶滤波器

$$R_{ij} = min \begin{cases} X_{i,j+1} + X_{i,j-1} - 2X_{ij}, \\ X_{i-1,j} + X_{i+1,j} - 2X_{ij} \\ X_{i-1,j+1} + X_{i+1,j-1} - 2X_{ij} \end{cases} (\square)$$

2024/11/24 信息隐藏与数字水印 14

残差(EDGE3x3)

EDGE3x3滤波器

$$\begin{bmatrix} -1 & +2 & -1 \\ \blacksquare & \blacksquare & \blacksquare \end{bmatrix}$$

垂直: -

$$R_{ij} = 2X_{i+1,j} + 2X_{i,j-1} + 2X_{i-1,j} - X_{i-1,j-1} - X_{i+1,j-1} - 4X_{ij} \quad (\Box)$$

水平: ↵

$$R_{ij} = 2X_{i,j+1} + 2X_{i,j-1} + 2X_{i-1,j} - X_{i-1,j-1} - X_{i-1,j+1} - 4X_{ij} \pmod{\mathbb{N}}$$

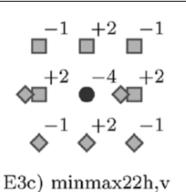
E3a) spam14h,v

E3b) minmax24

 $R_{ij} = min \begin{cases} 2X_{i,j+1} + 2X_{i,j-1} + 2X_{i-1,j} - X_{i-1,j-1} - X_{i-1,j+1} - 4X_{ij}, \\ 2X_{i-1,j} + 2X_{i,j-1} + 2X_{i+1,j} - X_{i-1,j-1} - X_{i+1,j-1} - 4X_{ij} \end{cases}$

残差(EDGE3x3)

EDGE3x3滤波器



$$R_{ij} = min \begin{cases} 2X_{i,j+1} + 2X_{i,j-1} + 2X_{i-1,j} - X_{i-1,j-1} - X_{i-1,j+1} - 4X_{ij}, \\ 2X_{i,j+1} + 2X_{i,j-1} + 2X_{i+1,j} - X_{i+1,j-1} - X_{i+1,j+1} - 4X_{ij} \end{cases}$$

垂直: 🗸

$$R_{ij} = min \begin{cases} 2X_{i+1,j} + 2X_{i,j-1} + 2X_{i-1,j} - X_{i-1,j-1} - X_{i+1,j-1} - 4X_{ij}, \\ 2X_{i,j+1} + 2X_{i-1,j} + 2X_{i+1,j} - X_{i+1,j+1} - X_{i-1,j+1} - 4X_{ij} \end{cases},$$

$$R_{ij} = min \begin{cases} 2X_{i,j+1} + 2X_{i,j-1} + 2X_{i-1,j} - X_{i-1,j-1} - X_{i-1,j+1} - 4X_{ij}, \\ 2X_{i,j+1} + 2X_{i,j-1} + 2X_{i-1,j} - X_{i+1,j-1} - X_{i+1,j+1} - 4X_{ij}, \\ 2X_{i,j+1} + 2X_{i+1,j} + 2X_{i-1,j} - X_{i+1,j+1} - X_{i-1,j+1} - 4X_{ij}, \\ 2X_{i,j-1} + 2X_{i+1,j} + 2X_{i-1,j} - X_{i+1,j-1} - X_{i-1,j-1} - 4X_{ij}, \end{cases}$$

2024/11/24 信息隐藏与数字水印 16

残差(EDGE5x5)

EDGE5x5滤波器

水平: 4

$$R_{ij} = 8(X_{i,j+1} + X_{i,j-1} + X_{i-1,j}) - 6(X_{i-1,j-1} + X_{i-1,j+1})$$

$$+ 2(X_{i-2,j-1} - X_{i-2,j} + X_{i-2,j+1})$$

$$+ 2(X_{i-1,j-2} - X_{i,j-2}) + 2(X_{i-1,j+2} - X_{i,j+2})$$

$$- (X_{i-2,j+2} + X_{i-2,j-2}) - 12X_{ij}$$

残差(EDGE5x5)

EDGE5x5滤波器

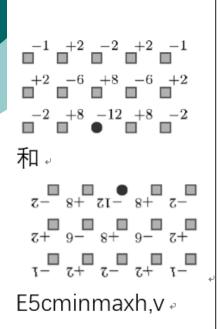
$$R_{ij}^{0} = 8(X_{i,j+1} + X_{i,j-1} + X_{i-1,j}) - 6(X_{i-1,j-1} + X_{i-1,j+1}) + 2(X_{i-2,j-1} - X_{i-2,j} + X_{i-2,j+1}) + 2(X_{i-1,j-2} - X_{i,j-2}) + 2(X_{i-1,j+2} - X_{i,j+2}) - (X_{i-2,j+2} + X_{i-2,j-2}) - 12X_{ij}$$

$$R_{ij}^{-\pi/2} = 8(X_{i,j-1} + X_{i-1,j} + X_{i+1,j}) - 6(X_{i-1,j-1} + X_{i+1,j-1}) + 2(X_{i-1,j-2} - X_{i,j-2} + X_{i+1,j-2}) + 2(X_{i-2,j-1} - X_{i-2,j}) + 2(X_{i+2,j-1} - X_{i+2,j}) - (X_{i-2,j-2} + X_{i+2,j-2}) - 12X_{ij}$$

$$R_{ij} = min\{R_{ij}^{0}, R_{ij}^{-\pi/2}\}_{i}$$

残差(EDGE5x5)

EDGE5x5滤波器



水平: $R_{ij}^{0} = 8(X_{i,j+1} + X_{i,j-1} + X_{i-1,j}) - 6(X_{i-1,j-1} + X_{i-1,j+1}) + 2(X_{i-2,j-1} - X_{i-2,j} + X_{i-2,j+1}) + 2(X_{i-1,j-2} - X_{i,j-2}) + 2(X_{i-1,j+2} - X_{i,j+2}) - (X_{i-2,j+2} + X_{i-2,j-2}) - 12X_{ij}$ $R_{ij}^{-\pi} = 8(X_{i,j+1} + X_{i,j-1} + X_{i+1,j}) - 6(X_{i+1,j-1} + X_{i+1,j+1}) + 2(X_{i+2,j-1} - X_{i+2,j} + X_{i+2,j+1}) + 2(X_{i+1,j-2} - X_{i,j-2}) + 2(X_{i+1,j+2} - X_{i,j+2}) - (X_{i+2,j+2} + X_{i+2,j-2}) - 12X_{ij}$ $R_{ij} = min\{R_{ij}^{0}, R_{ij}^{-\pi}\}_{\sigma}$

残差(EDGE5x5)

EDGE5x5滤波器

E5d minmax -

$$R_{ij}^{0} = 8(X_{i,j+1} + X_{i,j-1} + X_{i-1,j}) - 6(X_{i-1,j-1} + X_{i-1,j+1})$$

$$+ 2(X_{i-2,j-1} - X_{i-2,j} + X_{i-2,j+1})$$

$$+ 2(X_{i-1,j-2} - X_{i,j-2}) + 2(X_{i-1,j+2} - X_{i,j+2})$$

$$- (X_{i-2,j+2} + X_{i-2,j-2}) - 12X_{ij}$$

$$R_{ij}^{-\pi/2} = 8(X_{i,j-1} + X_{i-1,j} + X_{i+1,j}) - 6(X_{i-1,j-1} + X_{i+1,j-1})$$

$$+ 2(X_{i-1,j-2} - X_{i,j-2} + X_{i+1,j-2})$$

$$+ 2(X_{i-2,j-1} - X_{i-2,j}) + 2(X_{i+2,j-1} - X_{i+2,j})$$

$$- (X_{i-2,j-2} + X_{i+2,j-2}) - 12X_{ij}$$

$$R_{ij}^{-\pi} = 8(X_{i,j+1} + X_{i,j-1} + X_{i+1,j}) - 6(X_{i+1,j-1} + X_{i+1,j+1})$$

$$+ 2(X_{i+2,j-1} - X_{i+2,j} + X_{i+2,j+1})$$

$$+ 2(X_{i+1,j-2} - X_{i,j-2}) + 2(X_{i+1,j+2} - X_{i,j+2})$$

$$- (X_{i+2,j+2} + X_{i+2,j-2}) - 12X_{ij}$$

$$R_{ij} = min\{R_{ij}^{0}, R_{ij}^{-\pi/2}, R_{ij}^{-\pi}\}$$

残差(SQUARE)

SQUARE滤波器

$$R_{ij} = 2X_{i,j+1} + 2X_{i,j-1} + 2X_{i-1,j} + 2X_{i+1,j} - X_{i-1,j-1} - X_{i+1,j-1} - X_{i-1,j+1} - X_{i+1,j+1} - 4X_{ij}$$

$$\begin{bmatrix} -1 & +2 & -2 & +2 & -1 \\ +2 & -6 & +8 & -6 & +2 \\ -2 & +8 & -12 & +8 & -2 \\ -2 & -6 & +8 & -6 & +2 \\ -1 & -6 & +8 & -6 & +2 \\ -1 & +2 & -2 & +2 & -1 \\ -1 & -2 & -2 & +2 & -1 \\ -1 & -2 & -2 & -2 & -2 \\ -1 & -2 & -2 & -2 \\ -1 & -2 & -2 & -2 & -2 \\ -1 & -2 & -2 & -2 & -2 \\ -1 & -2 & -2 & -2 & -2 \\ -1 & -2 & -2 & -2 & -2 \\ -1 & -2 & -2 & -2 & -2 \\ -1 & -2 & -2 & -2 & -2 \\ -1 & -2 & -2 & -2 & -2 \\ -1 & -2 & -2 & -2 & -2 \\ -1 & -2 & -2 & -2 & -2 \\ -1 & -2 & -2 & -2 & -2 \\ -1 & -2 & -2 & -2 & -2 \\ -1 & -2 & -2 & -2 & -2 \\ -1 & -2 & -2 & -2 \\ -1 & -2 & -2 & -2 & -2 \\ -1 & -2 & -2 & -2 & -2 \\ -1 & -2 & -2 & -2 & -2 \\ -1 & -2 & -2 & -2 & -2 \\ -1 & -2 & -2 & -2 \\ -1 & -2 & -2 & -2 \\ -1 & -2 & -2 & -2 \\ -1 & -2 & -2 & -2 \\ -1 & -2 & -2 & -2 \\ -1 & -2 & -2 & -2 \\ -1 & -2 & -2 & -2 \\ -1 & -2 & -2 & -2 \\ -1 & -2 & -2 & -2 \\ -1 & -2 & -2 & -2 \\ -$$

$$R_{ij} = 8(X_{i,j+1} + X_{i,j-1} + X_{i-1,j} + X_{i+1,j}) - 6(X_{i-1,j-1} + X_{i+1,j-1} + X_{i-1,j+1} + X_{i+1,j+1}) + 2(X_{i-2,j-1} - X_{i-2,j} + X_{i-2,j+1}) + 2(X_{i+2,j-1} - X_{i+2,j} + X_{i+2,j+1}) + 2(X_{i-1,j-2} - X_{i,j-2} + X_{i+1,j-2}) + 2(X_{i-1,j+2} - X_{i,j+2} + X_{i+1,j+2}) - (X_{i-2,j+2} + X_{i-2,j-2} + X_{i+2,j-2} + X_{i+2,j+2}) - 12X_{ij} + 1$$

量化和截断

- $R_{ij} \leftarrow trunc_T \left(round \left(\frac{R_{ij}}{q} \right) \right)$
- 残差先以步长q量化。量化是为了使图像的不连续区域的残差,例如边缘和纹理残差,对隐写更敏感。
- 量化后的残差还需要截断。后续步骤需要计算量化残差的共生矩阵,截断可以抑制量化残差的动态范围,降低共生矩阵的规模。

SRM中, T取值为2, 因此共有 (2T+1)^4=625种矢量。 Z为 归一化因子, 使得C的所有元素 之和为1。 共生矩阵也可从垂直 方向扫描。

共生矩阵

共生矩阵用于描述相关性的变化, 定义如下:

$$\mathbf{C}_{\mathbf{d}}^{(h)} = \frac{1}{Z} \Big| \{ (R_{ij}, R_{i,j+1}, R_{i,j+2}, R_{i,j+3}) \Big|$$

$$R_{i,j+k-1} = d_k, k = 1, \dots, 4 \} \Big|$$

$$\sum_{\mathbf{d} \in \mathcal{T}_4} \mathbf{C}_{\mathbf{d}}^{(h)} = 1$$

$$\mathbf{d} = (d_1, d_2, d_3, d_4) \in \mathcal{T}_4 \stackrel{\triangle}{=} \{ -T, \dots, T \}^4,$$

其他要点

计算残差时,如果图像旋转90度前后,计算所得残差不变,那么称残差没有方向性 (nondirectional)。

共生矩阵对称性

- ○水平方向扫描所得共生矩阵(记为Ch),和垂直方向扫描所得 共生矩阵(记为Cv),两者之和为矩阵C(即C=Ch+Cv)。如这 个新矩阵C对图像具有旋转不变性(旋转90度前后,产生的矩阵 C相同),那么称残差具有h,v对称性。
- ○显而易见,不具方向性的残差,一定具有h,v对称性。部份具有 方向性的残差,也具有h,v对称性。
- 不考虑共生矩阵对称性时,共有78个共生矩阵,每个共生矩阵625维。综合考虑各类对称性,去除冗余后,SRM特征维度降为12753维。