




矩阵的PLUS分解及其应用

郝鹏威

北京大学信息科学中心

Queen Mary, University of London

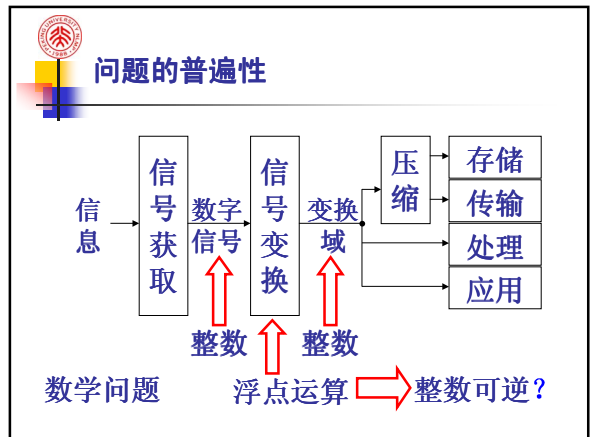
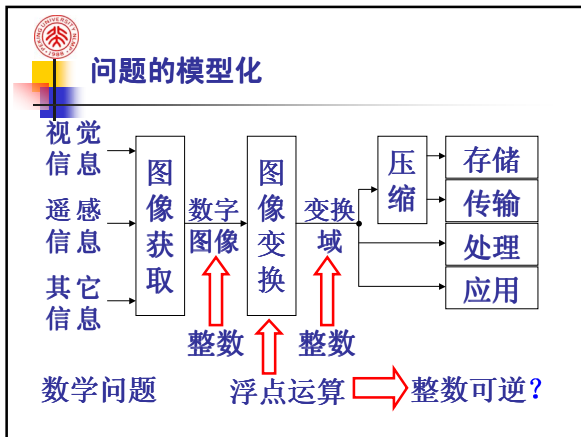
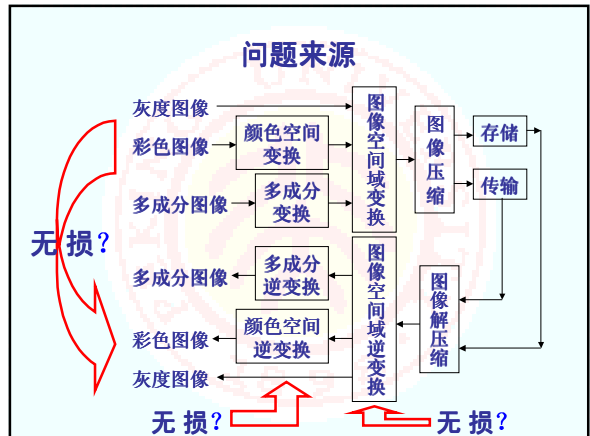


报告内容

- 一、背景介绍
- 二、研究成果
- 三、应用举例
- 四、问题公开



一、背景介绍



什么是整数可逆变换?

- 如果变换使某个定义域的任意整数 x 变换为整数 y , 其对应逆变换可以将整数 y 变换还原为整数 x
- 如果逆变换也要求是整数可逆的, 整数可逆变换就必须是一一对应的整数映射。

一个简单的例子

一个简单二维变换:
$$\begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} 4 & \\ & 1/4 \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$$

如果直接取整实现变换:

$$\left. \begin{aligned} \begin{bmatrix} 4 & \\ & 1/4 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} &\Rightarrow \begin{bmatrix} 4 \\ 0 \end{bmatrix} \\ \begin{bmatrix} 4 & \\ & 1/4 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 1 \end{bmatrix} &\Rightarrow \begin{bmatrix} 4 \\ 0.25 \end{bmatrix} \end{aligned} \right\} \Rightarrow \text{取整} \Rightarrow \begin{bmatrix} 4 \\ 0 \end{bmatrix}$$

变换结果并不是一对一的, 因此不可能整数可逆!

提高精度可以实现吗?

2000年NASA为实现无损变换还在研究高维线性变换后取整精度的确定问题

他们的实验发现即使取到小数点后几位都不能保证变换是整数可逆的, 而且付出的代价很大 (1bit/bit)!

直接可逆整数变换的可能性

通过直接取整实现的整数变换:

$$y = Ax + b \Rightarrow \hat{y} = [Ax + b]$$

假设取整误差为:

$$e = y - \hat{y} = y - [Ax + b] = Ax + b - [Ax + b]$$

并假设取整是整数独立的: $[n + c] = n + [c]$
 则相应的变换矩阵必须满足:

$$x = [A^{-1}(\hat{y} - b)] = [A^{-1}(Ax + b - e - b)] = [x - A^{-1}e] = x + [-A^{-1}e]$$

即: $[-A^{-1}e] = 0$ 或 $\|A^{-1}\|_{\infty} \leq 1$
 如果逆变换也是整数可逆的, 则还需要满足: $\|A\|_{\infty} \leq 1$
 因为存在: $\|A\|_{\infty} \|A^{-1}\|_{\infty} \geq \|AA^{-1}\|_{\infty} = 1$
 所以必然有: $\|A\|_{\infty} = \|A^{-1}\|_{\infty} = 1$
 这一条件是很苛刻的。

整数变换研究背景介绍


- 拼凑的小波变换整数实现:
 - S变换(Blume & Fand, 1989)
 - TS变换(Zandi et al, 1995)
 - S+P变换(Said & Pearlman, 1996)
- 梯状结构 (Bruekers & van den Enden, 1992)
- 提升方案 (二维, Sweldens, 1996)
- 凑的可逆颜色空间变换 (Gormish et al, 1997)
- 小波变换的分解 (二维, 石青云, 1998, Daubechies et al, 1998)

高维的线性变换如何实现?

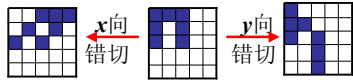
是否可以采用拼凑的方法设计?

没有理论指导是不可能的!

我们的解决办法: 矩阵分解

 **在图形学中的问题**


- 错切变换的实现可以在存储器级别进行，可以用一维的存储器复制来实现。



- 图形学中的投影变换用齐次坐标表示时，其变换可以用一个矩阵表示。
- 问题：能否及怎样把投影变换分解为一些错切变换以实现变换加速？


 **错切分解研究背景介绍**

- 二维旋转变换的两个错切-比例分解 (Catmull & Smith, SIGGRAPH, 1980)
- 二维旋转变换的三个错切分解 (Paeth, 1986)
- 三维仿射变换的三个错切-比例分解 (Hanrahan, SIGGRAPH, 1990)
- 三维旋转变换的三个错切分解 (Wittenbrink & Somani, SIGGRAPH, 1993)
- 三维投影变换的一个错切和二维变形分解 (Lacroute & Levoy, SIGGRAPH, 1994)
- 三维旋转变换的四个错切分解 (Chen & Kaufman, 2000)

 **错切分解与整数可逆分解的联系**

- 错切变换矩阵实际上等价于一个单位三角矩阵。
- 三维任意投影变换的错切分解问题就是一个单位三角分解问题
- 错切分解与我们用于整数变换的三角分解属于同一数学问题：可定制分解

 **二、研究成果**

 **单个整数变换可逆的条件**


如果任意整数 x 和 y 同时满足

$$y = ax + b$$

$$x = (y - b)/a$$

则 a , b , $1/a$ 和 b/a 都必须是整数

整数的 b 可以用取整来实现: $[b]$
 a 和 $1/a$ 则必须是特殊的整数：整数因子

 **整数因子**

- 整数域的单位群
- 整数因子: j
 - 实数: $1, -1$
 - 复数: $1, -1, i, -i$
- 整数可逆变换实现: $y = jx + [b]$
- 性质1: 整数因子不改变整数的大小
- 性质2: 整数因子的逆仍然是整数因子

单个整数可逆变换的基本计算结构

$y = jx + [b]$ $x = (1/j) \cdot (y + [b])$

- 整数因子: j
- 取整方法: 截尾、四舍五入等等, 十分灵活
- 前人方法的广义化: $j=1$ 时, 该结构与 Bruekers & van den Enden 的梯状结构和 Sweldens 的提升结构相同。

线性变换的实现方法

- 与单个整数的变换相同: $y = jx + [b]$
- 对矩阵的要求:
 - 对角线元素应该是整数因子
 - 对于正变换, 其它元素的计算必须完全包括在 b 内, 而且必须完全独立于 x
 - 对于逆变换, 其它元素的计算必须完全包括在 b 内, 而且必须完全独立于 y
- 基本可逆矩阵 (ERM)

变换直接整数可逆的矩阵形式

- 对角元素都是整数因子的基本可逆矩阵
- 三角基本可逆矩阵 (TERM)
 - 上三角基本可逆矩阵
 - 下三角基本可逆矩阵
- 单行基本可逆矩阵 (SERM)
 - $S_m = J + e_m s_m^T$
 - 只有一行非对角线元素不全为0
- 其它仅通过行列置换就可以转化为三角基本可逆矩阵的矩阵

TERM的性质

- 两个上TERM的积还是一个上TERM
- 两个下TERM的积还是一个下TERM
- TERM的逆还是一个TERM
- TERM的行列式值是一个整数因子

TERM的计算

- 上TERM计算: $m = 1, 2, 3, \dots, N-1$

$$\begin{cases} y_m = j_m x_m + \left[\sum_{n=m+1}^N a_{mn} x_n \right] = j_m x_m + [b_m] \\ y_N = j_N x_N \end{cases}$$
- 上TERM逆变换:

$$\begin{cases} x^N = y^N / j^N \\ x^m = (1/j^m) \cdot \left(y^m - \left[\sum_{n=m+1}^N a^{mn} x^n \right] \right) = (1/j^m) \cdot (y^m - [b^m]) \end{cases}$$
- 下TERM类似, 只是计算次序不同

单行基本可逆矩阵 (SERM)

- $S_m = J + e_m s_m^T$
- 性质:
 - 两个同一行的SERM积还是一个SERM
 - SERM的逆还是一个SERM
 - SERM的行列式值是一个整数因子

两种特殊矩阵的分解

- 旋转变换:

$$\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ (1-\cos\theta)/\sin\theta & 1 \end{bmatrix} \begin{bmatrix} 1 & -\sin\theta \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ (\cos\theta-1)/\sin\theta & 1 \end{bmatrix}$$
- 比例变换:

$$\begin{bmatrix} \alpha & 0 \\ 0 & 1/\alpha \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1/\alpha-1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ \alpha-1 & 1 \end{bmatrix} \begin{bmatrix} 1 & -1/\alpha \\ 0 & 1 \end{bmatrix}$$

一般矩阵如何分解

- 对任意可逆矩阵都存在LDU分解: $A=PLDU$
- 问题: 置换矩阵P, 单位三角矩阵L和U都可以实现整数可逆变换, 如何处理D?

$$\lambda_m = d_1 d_2 \cdots d_m \quad D_R = \text{diag}(1, \dots, 1, \lambda_N)$$

$$D = \text{diag}(d_1, d_2, \dots, d_N) = D_O \cdot D_E \cdot D_R = D_E \cdot D_O \cdot D_R$$

$$D_O = \begin{cases} \text{diag}(\lambda_1, 1/\lambda_1, \lambda_3, 1/\lambda_3, \dots, \lambda_{N-1}, 1/\lambda_{N-1}) & \text{if } N \text{ is even} \\ \text{diag}(\lambda_1, 1/\lambda_1, \lambda_3, 1/\lambda_3, \dots, \lambda_{N-2}, 1/\lambda_{N-2}, 1) & \text{if } N \text{ is odd} \end{cases}$$

$$D_E = \begin{cases} \text{diag}(1, \lambda_2, 1/\lambda_2, \lambda_4, 1/\lambda_4, \dots, \lambda_{N-2}, 1/\lambda_{N-2}, 1) & \text{if } N \text{ is even} \\ \text{diag}(1, \lambda_2, 1/\lambda_2, \lambda_4, 1/\lambda_4, \dots, \lambda_{N-1}, 1/\lambda_{N-1}) & \text{if } N \text{ is odd} \end{cases}$$
- 分解为7个TERM $A = PLV_1 V_2 V_3 V_4 V_5 V_6 V_7 D_R U$
 $= PV_1 V_2 V_3 V_4 V_5 V_6 V_7 D_R U$

分解矩阵的个数最少是几个?

- 我们证明: 最多可以不超过3个TERM的分解

$$A = PLUS_0 D_R$$

的充要条件是

$$\det P^T A = \det D_R \neq 0$$

其中

$$D_R = \text{Diag}(1, 1, \dots, 1, \det(P^T A))$$

$$S_0 = I + e_N s_0^T = I + e_N \cdot [s_1, s_2, \dots, s_{N-1}, 0]$$

证明概要

引理: 矩阵A存在单位三角分解A=LU的充要条件是A的所有顺序主子式都为1。

证明PLUSD存在的条件是矩阵可逆: 假设 $A = [a_1, a_2, \dots, a_N]$

$$AS_0^{-1} = [a_1, a_2, \dots, a_N] \cdot (I - e_N s_0^T) = [a_1 - s_1 a_N, a_2 - s_2 a_N, \dots, a_{N-1} - s_{N-1} a_N, a_N]$$

$$\det(AS_0^{-1})_k = \det[a_1 - s_1 a_N, a_2 - s_2 a_N, \dots, a_k - s_k a_N, a_k]$$

$$= \det[a_1 - s_1 a_N, a_2 - s_2 a_N, \dots, a_k] - s_k \det[a_1, a_2, \dots, a_{k-1}, a_N]_k$$

存在P使 $\det(P^T \cdot [a_N, a_1, a_2, \dots, a_{N-1}])_k \neq 0$ 或 $\det(P^T [a_1, a_2, \dots, a_{k-1}, a_N])_k \neq 0$

从而保证 $s_k (k=1, 2, 3, \dots, N-1)$ 都存在:

SERM分解

存在等式:

$$\begin{bmatrix} A^{11} & A^{12} \\ A^{21} & A^{22} \end{bmatrix} = \begin{bmatrix} I & 0 \\ A^{21} A^{11} & A^{22} - A^{21} A^{11} A^{12} \end{bmatrix} \begin{bmatrix} A^{11} & A^{12} \\ 0 & I \end{bmatrix}$$

$$\det \begin{bmatrix} A^{11} & A^{12} \\ A^{21} & A^{22} \end{bmatrix} = \det(A^{22} - A^{21} A^{11} A^{12}) \cdot \det(A^{11})$$

因此, 利用TERM分解A=PLUS₀就有:

$$A = PS_N S_{N-1} \cdots S_1 S_0$$

$$LU = \begin{pmatrix} LUS_1^{-1} \\ LUS_2^{-1} \\ \dots \\ LUS_N^{-1} \end{pmatrix} \begin{pmatrix} S_1 \\ S_2 \\ \dots \\ S_N \end{pmatrix}$$

可以分解为基本可逆矩阵的充要条件

矩阵行列式值的绝对值为1。

比直接取整变换可逆的条件要宽松得多



如果矩阵行列式值的绝对值不为1

只要矩阵可逆，可对原变换矩阵进行修正：

乘一对角阵或一非零常数。

矩阵修正还可以使：

- 分解的基本可逆矩阵数目最少
- 变换域的动态范围得到控制
- 变换的计算效率提高
-



基本可逆矩阵分解算法

1. 分解为三个三角基本可逆矩阵 (**TERM**分解) : 类似于普通三角分解的计算方法
2. 进一步分解为单行基本可逆矩阵 (**SERM**分解) : 从变换矩阵中逐行提取

例：

$$\begin{bmatrix} 2 & 3 \\ 3 & 4 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 1/2 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 4 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 1/2 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 2 & 0 \\ 2 & 1/2 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 2 & -1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1/2 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & -1/2 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}$$



计算复杂度比较

Implementation	Addition	Multiplication	Rounding	Permutation
Original Transform	$N^2 - N$	N^2	N	No
TERM factorization	$N^2 - 1$	$N^2 - 1$	$2N - 1$	Needed
SERM factorization	$N^2 - 1$	$N^2 - 1$	$N + 1$	Needed

采用分解后基本可逆矩阵变换的总计算复杂度与原变换的计算复杂度相近，不增加。



TERM分解的误差

$$A = PLUS_0$$

$$u = P \cdot (u_1 + L \cdot (u_2 + Uu_3)) = P(u_1 + Lu_2 + LUu_3)$$

$$|u| = |P(u_1 + Lu_2 + LUu_3)| \leq P(|u_1| + |Lu_2| + |LUu_3|)$$

$$\|u\|_{\infty} \leq u \cdot (1 + \|L\|_{\infty} + \|LUe_N\|_{\infty})$$



基本可逆矩阵分解的一些特点

- 分解不唯一
- 实矩阵的分解还是实的
- 三角基本可逆矩阵分解数目不大于3
- $N \times N$ 矩阵的单行基本可逆矩阵分解数目不大于 $N+1$
- 误差上界只与变换矩阵的分解有关



基本可逆矩阵分解的优点

- 性能保持：原线性变换非常好的近似
- 整数可逆：变换无损
- 取整方式灵活：截尾，四舍五入，或其它
- 原位计算：加法赋值 (+=)
- 逆变换简单：减法赋值 (-=)
- 计算复杂度：加法和乘法次数为 $N^2 - 1$

更一般的三角分解

- A 为一般可逆矩阵
- P 用一个三角矩阵代替 \rightarrow 伪置换矩阵
- U 的对角线元素任意 \rightarrow 用户可自由给定
- S 的形式多种多样 \rightarrow 用户可自由选择

\downarrow

PLUS分解: $A=PLUS$
可定制三角分解
customizable triangular factorization

特殊矩阵S的形式

- 单行基本可逆矩阵
- 单列基本可逆矩阵
- 单位双对角矩阵
- 其他.....?

分块矩阵的分解

- 分块矩阵分解是元素矩阵分解的推广
- 为实现并行和高效的计算
- 难点: 分块矩阵中有的块可能并不可逆
- 问题: 如何分块? 如何置换? 怎样分解的计算效率更高?
- 解决办法: 定义行列式矩阵函数

\downarrow

BLUS分解(余轶原)

已经解决的矩阵分解问题的范围

线性变换 \supset A 可逆 \supset $|\det A|=1$ \supset $\|A\|_\infty = \|A^{-1}\|_\infty = 1$

发表相关论文

几篇重要的期刊论文:

郝鹏威、石青云: “可逆线性变换的整数实现”, *中国科学 (E辑)*, 2000年, 第30卷, 第2期, 132-141页。

郝鹏威、石青云: “Matrix Factorization for Reversible Integer Mapping”, *IEEE Transactions on Signal Processing*, V49, N10, 2314-2324, Oct. 2001.

余轶原、郝鹏威: “均匀分块矩阵的分块TERM分解”, *中国科学 (E辑)*, 已接受

郝鹏威: “Customizable Triangular Factorizations of Matrices”, *Linear Algebra and Its Applications*, 已接受

新的图像压缩国际标准JPEG 2000建议书:

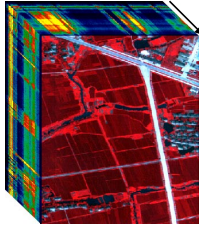
郝鹏威、石青云: “Proposal of Reversible Integer Implementation for Multiple Component Transforms”, *ISO/IEC JTC1/SC29/WG1N 1720*, Arles, France, July 2000. (此建议已被采纳并进入国际标准的最终文本)

JPEG 2000

Part	Title	CFP	WD	CD	FCD	FDIS	IS
1	JPEG 2000 Image Coding System: Core Coding System	97/03	99/03	99/12	00/03	00/10	00/12
2	JPEG 2000 Image Coding System: Extensions	97/03	00/03	00/08	00/12	01/07	01/10
3	Motion JPEG 2000	99/12	00/07	00/12	01/03	01/07	01/10
4	Conformance Testing	99/12	00/07	00/12	01/07	02/02	02/05
5	Reference Software	99/12	00/03	00/07	00/12	01/08	01/11
6	Compound Image File Format	97/03	00/12	01/03	01/11	02/03	02/05

- CFP: Call for Proposals
- WD: Working Draft
- CD: Committee Draft
- FCD: Final Committee Draft
- FDIS: Final Draft International Standard
- IS: International Standard

例 2：多成分变换



多成分之间去相关变换：

- 离散小波变换 (DWT)
- TM图像的缨帽变换
- 主成分分析变换(KL变换)
- 离散余弦变换 (DCT)
-

变换域的JPEG 2000压缩

多成分图像数据

例 2：多成分图像压缩

前人的方法：

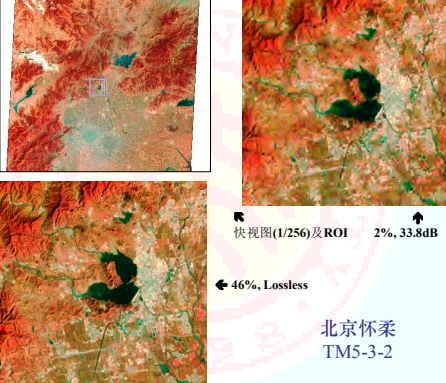
- 有损压缩和无损压缩采用不同的方法
- 一定精度的有损变换与误差的无损编码相结合

多成分变换矩阵有可能是十分巨大的，采用拼凑方法来设计一个近似的整数可逆实现是不可能的！

我们的解决方案 (JPEG 2000的1720号提案)：

用矩阵分解实现多成分变换的整数可逆 (包括KLT)

例 3：基于感兴趣区域图像压缩



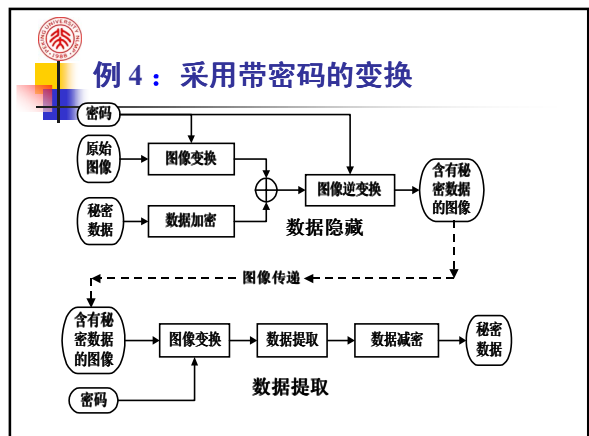
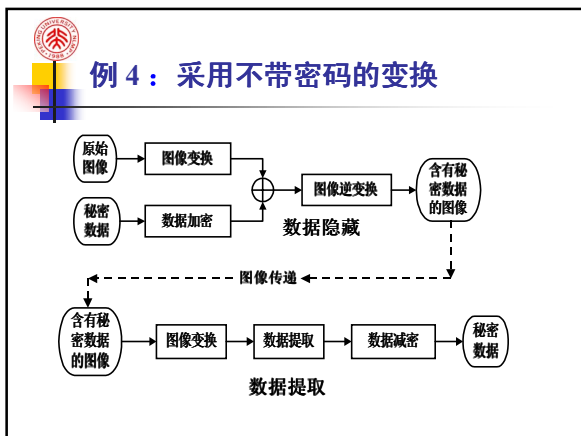
北京怀柔
TM5-3-2

快视图(1/256)及ROI 2%, 33.8dB

46%, Lossless

可逆整数变换在信息安全中的应用

- 带有密码的变换：变换具一些有良好的性质（如正交），同时又含有密码
- 隐蔽通信：把秘密数据隐藏在一个本身有含义的信号中实现的通信
- 数字水印：用于保护版权、及来源认定



例 8：体数据（图像）匹配加速

- 以一幅图像为基准对另一幅图像频繁迭代使用几何变换（仿射变换）以寻找最佳匹配方向和位置。

应用PLUS分解的优势

- 变换针对每一行/列/层数据点计算其变换后的新位置（加速至少O(N)倍）
- 不用插值就可以得到所有点
- 变换过程一般无需额外的数据空间
- 变换后的数据可以完全无损恢复

四、问题公开

1. PLUS分解中S的一般形式

我们对PLUS分解中的特殊矩阵S只证明了几种形式下的充要条件，只发现了两个必要条件和一个充分条件

但特殊矩阵S的一般形式到底要满足什么样的充要条件PLUS分解才存在？

2. 误差最小的PLUS分解

既然PLUS分解不唯一，而且取整误差的上界只与变换矩阵的分解有关

$$|u| = |P(u_1 + Lu_2 + LUu_3)| \leq P(|u_1| + |Lu_2| + |LUu_3|)$$

那么，取整误差最小的分解是什么？如何得到？矩阵分解中用什么规则去选主元？

3. PLUS分解的稳定性

当矩阵阶数太大时，PLUS分解就会出现不稳定的情形，L、U和S的一些元素值会突然增大。

PLUS分解出现不稳定的原因是什么？稳定和不稳定的边界条件是什么？如何使PLUS分解保持稳定？



4. PLUS分解的扰动分析

$$A=PLUS$$



$$A+dA = P(L+dL)(U+dU)(S+dS)$$

数据扰动对PLUS分解的影响有多大?

什么样的矩阵对扰动影响小?

分解前减小扰动的方法是什么?

分解过程中抵抗扰动的方法是什么?



5. PLUS分解的其它应用

随着对我们的矩阵PLUS分解理论的掌握和普及，我们坚信：新的应用领域一定会被不断发现，我们的理论成果必将会在更多的应用领域发挥更大的作用。



谢谢

phao@cis.pku.edu.cn

phao@dcs.qmul.ac.uk

<http://www.dcs.qmul.ac.uk/~phao>