矩阵三角分解在数字水印中的应用

王树梅[1,2],王志成[2],赵卫东[2]
WANG Shu-mei[1,2],WANG Zhi-cheng[2],ZHAO Wei-dong[2]

1.同济大学 CAD 研究中心,上海 201804
2.徐州师范大学 计算机学院,江苏 徐州 221000
1.CAD Research Center,Tongji University,Shanghai 201804,China
2.Computer Academy,Xuzhou Normal University,Xuzhou,Jiangsu 221000,China
E-mail:plum8@163.com

WANG Shu-mei,WANG Zhi-cheng,ZHAO Wei-dong.Gray scale watermarking algorithm based on LU factorization. Computer Engineering and Applications,2009,45(13):111-113.

Abstract: The method to decompose the non-singular matrix into two triangulars is a approach that can transform complex matrix into a simple matrix,and it is also the method of analyzing the characteristics of matrix.The digital image can be seen as a matrix,based on the characteristics of the LU Factorization,this paper presents a novel robust watermarking algorithm in wavelet domain of digital image.Firstly,the original image will be transformed into wavelet domain by DWT,and the level of which is decided by the volume of watermark information.Next to do is computing the variances of the last details,and selecting detail matrix information whose variance is the max one among details.Then it will be preprocessed,if the image matrix is singular matrix,it will be converted into a non-singular matrix by permutation matrix which can be as a key;Secondly,the preprocessed image is decomposed into two triangular matrices including the upper one and the lower one with 1's on the main diagonal,and which have good distribution;Finally,the scrambled meaningful watermark is embedded into the non-zero pixels of two triangular matrixes adaptively.The experimental results show that the algorithm is simple,with better robustness and security.
Key words: digital watermarking;singular matrix;triangular factorization;permutation matrix

摘 要:将非奇异矩阵进行三角分解是一种将复杂矩阵变换为简单矩阵的方法,也是分析矩阵特性的方法。而数字图像也可以看作矩阵,根据图像的这一特点结合小波变换提出一种鲁棒性较好的水印算法。首先对图像进行离散小波分解,分解的尺度由水印信息量大小决定;然后计算分解后最高尺度的细节矩阵的方差,选择方差最大的一个进行预处理,若其是奇异矩阵,通过一个置换矩阵将其转换为非奇异矩阵,这里置换矩阵可以当作密钥;然后对其进行 LU 分解,得到两个具有良好分布特性的三角矩阵;最后将置乱后的水印信息嵌入到两个矩阵的非零像素值中。实验结果证明该算法简单易行,具有较好的鲁棒性和安全性。
关键词:数字水印;奇异矩阵;三角分解;置换矩阵
DOI:10.3778/j.issn.1002-8331.2009.13.033 **文章编号:**1002-8331(2009)13-0111-03 **文献标识码:**A **中图分类号:**TP391

数字水印作为信息安全的一个主要内容,被越来越多的研究者所关注。因此数字水印的算法也层出不穷[1-4],水印算法可以分为两大类,一类是时-空域算法,另一类是变换域算法。由于时-空域算法一般都是根据载体图像的统计特征来嵌入水印,再就是根据位平面特点来嵌入水印,这样的算法容易被攻击,安全性得不到保证。所以现在大部分水印研究者都把目光转向了变换域,因为变换域的安全性较强。但是变换域仍然具有其本质的弱点,即在水印嵌入过程中会有误差出现,即会有部分数据丢失。

这里将空域和变换域结合起来,变换域使用具有多分辨能力的小波域, 空域的转换是利用矩阵里的具有良好特性的 LU 分解。实验结果证明算法具有良好的鲁棒性和安全性。

1 理论基础

1.1 离散小波变换

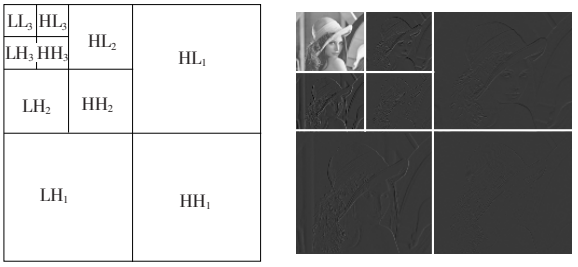
小波变换用于图像分析的基本思想就是把图像进行多分辨分解,将图像分解成不同空间、不同频率的子图像。图像经过小波变换后被分割成四个频带:水平、垂直、对角线和低频,低频信息还可以继续分解如图 1 所示。对一幅图像来说,小波变换构成了对它的多尺度时频分解, 图 1 给出了 lena 图像的两个尺度的分解。

左上角(LL2)是最低频段滤波后的低尺度逼近,同级分辨下,HL2 块包含了水平方向高通、垂直方向低通滤波后所保留的细节信息。同样的,LH2 块保留的是水平方向低通、垂直方向

基金项目:国家高技术研究发展计划(863)(the National High-Tech Research and Development Plan of China under Grant No.2005AA414020)。
作者简介:王树梅(1972-),女,博士研究生,讲师,主要研究领域为数字水印技术与图像处理等;王志成(1975-),男,同济大学 CAD 中心博士,研究方向为图像处理域智能控制;赵卫东(1964-),男,研究员,博导,主要研究领域为 CAD 及信息安全。
收稿日期:2008-03-06 **修回日期:**2008-05-15

高通滤波后所得的细节信息,块包含的是水平和垂直方向都经过高通滤波后的细节信息。相同的处理过程在中分辨率层和高分辨率层重复进行。

图像经过小波变换后生成的小波图像的数据总量与原图像的数据量相等，生成的小波图像具有与原图像不同的特性，表现在图像的能量主要集中于低频部分,而水平、垂直和对角线部分的能量则较少;水平、垂直和对角线部分表征了原图像在水平、垂直和对角线部分的边缘信息,具有明显的方向特性。



(a)图像的三级小波分解　(b)Lena 图像的二级小波分解

图 1　Lena 图像的小波分解

由图1(b)可见,LL 子带图像集中了原始图像的绝大多数能量,称为原始图像的逼近子图。子带图像 HL、LH 和 HH 分别保持了原始图像的水平边缘细节、垂直边缘细节和对角边缘细节,它们刻画了图像的细节特性,称为细节子图。逼近子图具有较强的抵抗外来影响的能力,稳定性好;边缘细节子图易受噪声、图像处理操作等的影响,稳定性较差。

1.2　矩阵的三角分解

矩阵三角分解分解是利用一些列的 Gaussian 顺序消元过程将矩阵 $\boldsymbol{A}$ 分解为两个三角矩阵的乘积,如下形式:

$$\boldsymbol{A}=\boldsymbol{LU} \tag{1}$$

这里 $\boldsymbol{A}$ 和 $\boldsymbol{L}$ 是 $M\times N$ 的矩阵,$\boldsymbol{U}$ 是 $N\times N$ 的矩阵,且 $\boldsymbol{L}$ 是主对角线上都是 1 的下三角矩阵,$\boldsymbol{U}$ 是上三角矩阵。

$\boldsymbol{A}$ 能够被分解为两个三角矩阵的前提条件就是 $\boldsymbol{A}$ 是 $\boldsymbol{A}$ 的前 $n-1$ 阶顺序主子式非零。如果这个条件不满足,可以将 $\boldsymbol{A}$ 进行预处理,将其转换为非奇异矩阵,方法就是给 $\boldsymbol{A}$ 左(或右)乘以置换矩阵 $\boldsymbol{P}$(以 n 阶单位矩阵的 n 个列向量为列做成的 n 阶矩阵),就可以把 $\boldsymbol{A}$ 的行(或列)的次序重新排列,使之满足这个条件,即有下式成立:

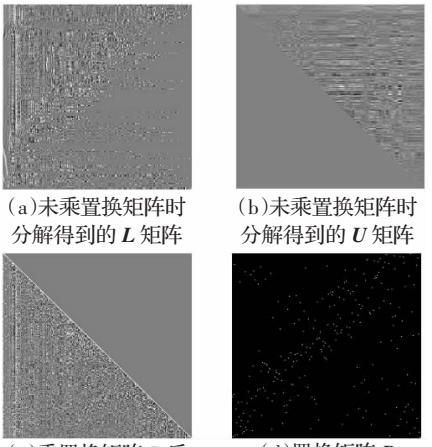
$$\boldsymbol{PA}=\boldsymbol{LU} \tag{2}$$

对一幅灰度图像 $D(m,n)$,$m=1\cdots M$,$n=1\cdots N$ 来说,可以看作一 $M\times N$ 矩阵,且每个元素都是非负的。但是图像一般都不是方阵,即图像矩阵的行数和列数不一样,这里不能判断其顺序主子式是否为零。且通过小波变换后的细节信息矩阵会有负值出现，但这都不影响对其进行三角分解。以下以仍然以 256×256 大小的 Lena 图像为例,进行说明。

这里将 8 位灰度图像矩阵转化为双精度矩阵并做归一化处理,然后做三角分解,分解后的结果如图 2 的(a)和(b)。显然图 2(a)所显示的 $\boldsymbol{L}$ 矩阵不是理想的结果,通过计算其行列式值为 0,即该矩阵为奇异矩阵,所以不能得到标准的下三角矩阵,需要将其左乘一置换矩阵 $\boldsymbol{P}$(图 2 的(d))。再将其做三角分解,结果如图 2(c),是一主对角线都为 1 的下三角矩阵。

若想得到原始图像矩阵可以将式(2)左右都乘以 $\boldsymbol{P}$ 的逆,即有下式:

$$\boldsymbol{P}^{-1}\boldsymbol{PA}=\boldsymbol{P}^{-1}\boldsymbol{LU} \tag{3}$$



(a)未乘置换矩阵时分解得到的 $\boldsymbol{L}$ 矩阵　(b)未乘置换矩阵时分解得到的 $\boldsymbol{U}$ 矩阵

(c)乘置换矩阵 $\boldsymbol{P}$ 后分解得到的 $\boldsymbol{L}$ 矩阵　(d)置换矩阵 $\boldsymbol{P}$

图 2　Lena 图像矩阵的三角分解

即:$\boldsymbol{A}=\boldsymbol{P}^{-1}\boldsymbol{LU}$　(4)

从以上分析 $\boldsymbol{LU}$ 分解具有良好的能量分布,给水印的嵌入位置的选择提供了较为明确的参考。因为水印一般都嵌入在非零像素值里,这样增强了水印的抗攻击性。而置换矩阵 $\boldsymbol{P}$ 作为密钥提高了水印的安全性。

2　水印系统

2.1　水印的嵌入

一般水印系统中,主要包括三大部分,一是水印的嵌入,二是水印的提取,三是对水印系统的攻击测试。在这三部分中,可以说每一部分都一个水印系统非常重要,但是嵌入过程决定了其他部分。选择嵌入思想决定了提取过程,也决定了攻击测试效果。

算法的嵌入步骤如下:

步骤 1　读入原始载体图像,并对其做预处理,若其为 8 位灰度图像,将其转化为双精度实数矩阵,便于后面的处理。

步骤 2　将步骤 1 得到的结果进行小波分解，分解的尺度大小由载体图像的大小和水印的信息量确定。

步骤 3　选择最高尺度的水平和垂直两个细节分量作为进一步处理的对象。

步骤 4　分别将步骤 3 得到的矩阵结果左乘置换矩阵 $\boldsymbol{PH}$ 和 $\boldsymbol{PV}$,使得乘得的结果都是非奇异矩阵。

步骤 5　将步骤 4 得到的结果进行 $\boldsymbol{LU}$ 分解,得到四个三角矩阵,分别是 $\boldsymbol{LH}$、$\boldsymbol{UH}$ 和 $\boldsymbol{LV}$、$\boldsymbol{UV}$,其中 $\boldsymbol{LH}$ 和 $\boldsymbol{LV}$ 主对角线都为 1 的下三角矩阵,$\boldsymbol{UH}$ 和 $\boldsymbol{UV}$ 为上三角矩阵。

步骤 6　利用步骤 4 和步骤 5 的方法将水印矩阵 $\boldsymbol{LU}$ 分解,会产生 $\boldsymbol{PW}$,$\boldsymbol{LW}$ 和 $\boldsymbol{UW}$,同样 $\boldsymbol{PW}$ 作为重构水印的密钥,不作为水印嵌入。

步骤 7　按如下规则嵌入水印

$$\boldsymbol{LH}=\boldsymbol{LH}+\alpha_1*(\boldsymbol{UW})' \tag{5}$$

$$\alpha_1=(mean(abs(\boldsymbol{LH}))/\max(abs(\boldsymbol{LH})))*0.1 \tag{6}$$

$$\boldsymbol{UV}=\boldsymbol{UV}+\alpha_2*(\boldsymbol{LW})' \tag{7}$$

$$\alpha_2=(mean(abs(\boldsymbol{UV}))/\max(abs(\boldsymbol{UV})))*0.1 \tag{8}$$

这里是将 $\boldsymbol{LW}$ 和 $\boldsymbol{UW}$ 的转置矩阵分别嵌入到 $\boldsymbol{LH}$ 和 $\boldsymbol{UV}$ 中,α_1 和 α_2 分别自适应于 $\boldsymbol{LH}$ 和 $\boldsymbol{UV}$ 的拉伸因子，其计算方法如式(6)和式(8)所示。Mean 函数是求平均函数,abs 功能是求绝对

值，max 是求最大值。

保存 ***PH***、***UH*** 和 ***PV***、***LV*** 用来提取水印。

（8）根据式（4）小波逆变换重构含水印图像，并进行保存。

因为 ***LU*** 分解不是唯一的[5]，所以为保证能够准确提取出水印，算法在水印嵌入的同时也产生了一些密钥矩阵。由式（4）可知，四个矩阵只要已知三个矩阵，其余一个就是唯一的。所以这里的置换矩阵和其中一个三角阵都被当作密钥，增加了算法的安全性，但是也增加了存储的成本。

另外，需要指出的是若水印信息值较大时，得到的含水印图像会出现板块现象，为了避免这一现象，也可以先将所选择的细节矩阵进行 8×8 分块再对每块进行 ***LU*** 分解。

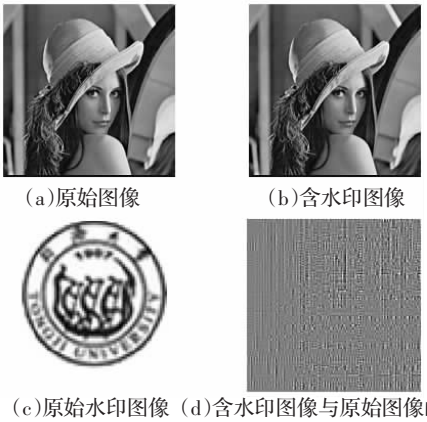
2.2　水印的提取

通常情况下，水印的提取过程都是嵌入过程的逆过程，但算法的提取过程不全是嵌入过程的逆过程。将含水印图像做与与嵌入过程同样的小波分解后，根据 ***PH***、***UH*** 和 ***PV***、***LV*** 找到嵌入水印的上三角矩阵和下三角矩阵，然后根据式（5）~（8）计算出水印的上三角矩阵和下三角矩阵，再结合 ***PW*** 重构水印图像。

因为仍然需要原始图像的参与，因此算法是非盲水印检测算法。值得注意的是在提取过程中，从 ***LH*** 里提取出来的是 ***UW***的转置，而从 *UV* 里提取出来的是 ***LW*** 的转置，需要再进行一次转置。

3　实验仿真与算法性能分析

这里采用纹理比较丰富的 Lena 图像作为载体，以徐州师范大学的 Logo 灰度图像作为水印。从图 3（b）可以看出，算法具有较好的不可见性，但人眼视觉是不能观察出图 3（a）和图 3（b）的差别的。而且这里选用的水印是使用范围比较广泛的有意义灰度图像（如图 3（c）），图 3（d）显示原始图像与载体图像之间的差别，即为嵌入的信息，从位置上可以看出水印都是嵌入在像素值比较大的像素中，即是人眼不敏感的地方，提高了水印的不可见性。



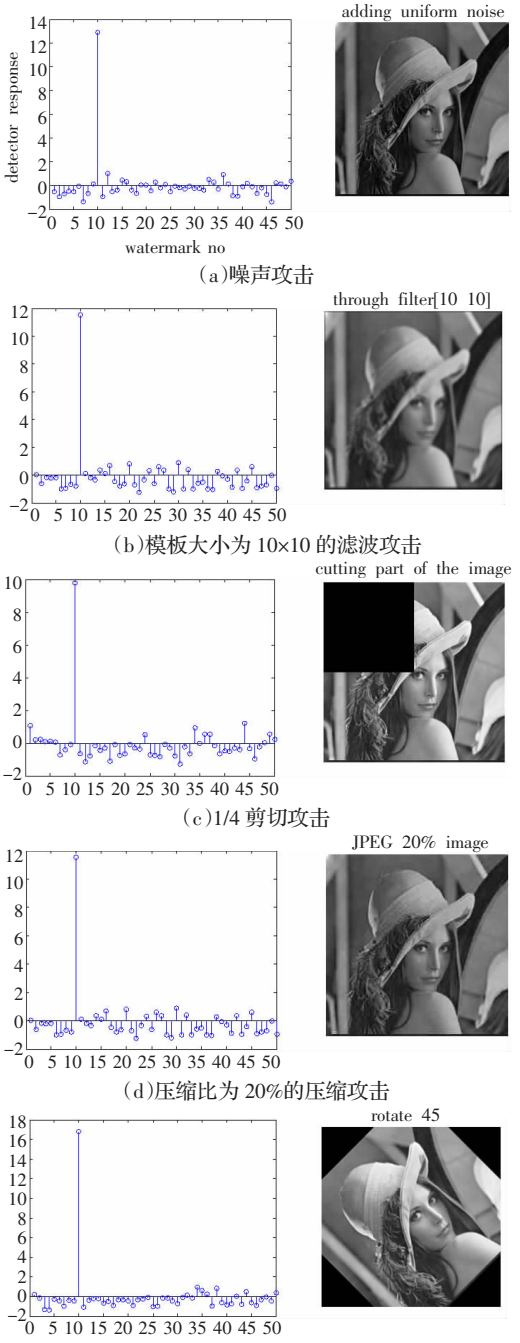
（a）原始图像　（b）含水印图像

（c）原始水印图像　（d）含水印图像与原始图像的差

图 3　Lena 图像嵌入水印

常见的图像攻击有添加噪声、滤波、剪切、压缩以及旋转，图 4 各图分别对对含水印图像做以上五种攻击，而且攻击程度比一般情况下要大。通过测试结果可知，不管哪一种攻击，提取出的水印与原始水印的相似程度比较明显，即不管哪一种攻击总有一个非常明显的最大值突出出来（图 4（a）~（e））。可见算法的抗攻击性较好，能够抵抗一般性强度较大的攻击。

为了更好地说明算法的良好的不可见性，将 Peppers、



（a）噪声攻击

（b）模板大小为 10×10 的滤波攻击

（c）1/4 剪切攻击

（d）压缩比为 20%的压缩攻击

（e）角度为 45°的旋转攻击

图 4　攻击测试（提取水印与原始水印的相关值图像与接受攻击的含水印图像）

Baboon、Cameraman 和 Fishboatng 作为载体进行实验，实验数据见表 1。从表 1 可知，对于不同的图像本算法仍然具有叫好的不可见性和鲁棒性。

表 1　不同图像的 PSNR 和 NC

	peppers	baboon	cameraman	fishingboat
PSNR	43.503 8	40.335 6	41.887 0	42.468 9
NC	0.987 5	0.976 2	0.996 3	0.985 9

$$PSNR=\frac{MN\ \max\limits_{m,n} I_{m,n}^{2}}{\sum\limits_{m,n}\left(I_{m,n}-I'_{m,n}\right)^{2}} \tag{9}$$

（下转 149 页）