# 基于矩阵 LU 分解的数字水印算法 [1]

牛少彰 钮心忻 杨义先

(北京邮电大学信息安全中心 北京 100876)

**摘 要:** 该文提出了一种新的基于矩阵 LU 分解的数字水印算法. 该方法首先将数字图像的非负矩阵表示转化为 G- 对角占优矩阵, 再进行 LU 分解, 通过量化函数进行数字水印的嵌入, 恢复水印时不需要原始图像. 将矩阵的 LU 分解数字水印算法与 DCT 的中频系数比较法进行了对比实验. 实验结果表明这种方法运算速度快并且具有很好的鲁棒性.

**关键词:** 信息隐藏, 数字水印, LU 分解

**中图分类号:** TP391 **文献标识码:** A **文章编号:** 1009-5896(2004)10-1620-06

# Digital Watermarking Algorithm Based on LU Decomposition

Niu Shao-zhang Niu Xin-xin Yang Yi-xian

(*Info. Security Center, Beijing Univ. of Posts and Telecom., Beijing* 100876, *China*)

**Abstract** In this paper, a new digital watermarking algorithm based on LU decomposition of matrix is proposed. In order to apply LU decomposition, the corresponding nonnegative matrix of the image is transformed into G-diagonally dominant matrix. In the course of embedding digital watermarking, the scale quantization function is used. The original image is not needed in the recover progress. Experiments are given for contrasting the LU algorithm with DCT mid-frequency coefficient comparison method, and results show that this new algorithm is robust and easy to embed and extract.

**Key words** Information hiding, Digital watermarking, LU decomposition

## 1 引言

随着计算机和网络技术的飞速发展, 使得数字化多媒体数据的复制和传送变得非常容易. 数字作品的完美复制和快速的网上传送, 为侵权者提供了便利, 因此数字产品的版权保护问题已经越来越引起了人们的关注. 在过去的几年里, 数字水印已经成为用来解决数字多媒体中版权问题和内容认证的主要工具. 例如, 对于图像来说, 为了保护版权, 在图像里加入一个水印(版权标志), 并且希望不要引起图像视觉上的降质. 一旦需要验证图像的所有权时, 可以通过算法提出水印来实现. 数字水印技术的发展为解决数字产品的侵权问题提供了一个有效的解决途径.

按照水印的嵌入方法可以将水印分为两类: 空间域水印和变换域水印. 空间域方法通过改变载体信息的空间域特性来隐藏水印; 最低有效位 (LSB) 方法是其中最具代表性的一种 [1,2], 其原理就是通过修改表示数字图像颜色 (或者颜色分量) 的较低位平面, 一般对于图像来说, 最低两比特位的修改不会给人的视觉造成很强的修改感觉. 即通过调整数字图像中对感知不重要的像素低比特位来表达水印信息, 达到嵌入水印信息的目的. 变换域方法通过改变数据 (主要指

[1] 2003-06-16 收到, 2003-08-21 改回
国家自然科学基金 (60073049), 国家杰出青年基金 (69425001), 国家重点基础研究发展规划项目 (1999035805) 和高校骨干教师项目资助课题

图像、音频、视频等) 变换域的一些系数来隐藏水印. 它在图像变换域改变数据，再进行反变换得到嵌入水印后的图像，基于变换域的数字水印算法主要有：离散余弦变换 (DCT) 、离散傅里叶变换 (DFT) 和离散小波变换 (DWT) 等 [3−5] .

本文提出一种新的基于矩阵 LU 分解的数字水印方法. 该算法是首先将表示数字图像的矩阵转化为 G−对角占优矩阵，再用矩阵的分解理论进行 LU 分解，将数字水印嵌入到分解后的矩阵中. 我们将这种方法与 DCT 中频系数的相邻系数比较法进行了比较，实验结果表明：基于矩阵 LU 分解的数字水印方法具有很好的鲁棒性并且嵌入和提取的速度快.

## 2 G−对角占优矩阵的 LU 分解

在矩阵的研究中，对角占优矩阵具有许多好的性质，因而在数值计算中有着广泛的应用. 下面将其推广到更为一般的情形.

**定义 1**　设函数 $f=(f_1,f_2,\cdots,f_n)$ ，其中 $f_i(i=1,2,\cdots,n)$ 为只与矩阵非对角元素的模有关的非负函数，若对于任意的 $n$ 阶矩阵 $\boldsymbol{A}=[a_{ij}]$ ，满足 $|a_{ii}|>f_i(\boldsymbol{A}),i=1,2,\cdots,n$ ，都有 $\boldsymbol{A}$ 是非奇异的，则称函数 $f=(f_1,f_2,\cdots,f_n)$ 是一个 G−函数.

引入下列表达式 $r_i(\boldsymbol{A})=\sum_{j=1,j\neq i}^{n}|a_{ij}|$ ，$c_i(\boldsymbol{A})=\sum_{j=1,j\neq i}^{n}|a_{ji}|$ ，$i=1,2,\cdots,n$ ，那么 $r=(r_1,r_2,\cdots,r_n)$ 和 $c=(c_1,c_2,\cdots,c_n)$ 是 G−函数，更一般地，设 $n$ 维列向量 $\boldsymbol{x}=[x_1\ \ x_2\ \cdots\ x_n]^{\mathrm{T}}$ 的每个分量都为正数，称这样的向量 $\boldsymbol{x}$ 为正向量，引入记号 $r_i^x(\boldsymbol{A})=\frac{1}{x_i}\sum_{j=1,j\neq i}^{n}|a_{ij}|x_j$ ，$c_i^x(\boldsymbol{A})=\frac{1}{x_i}\sum_{j=1,j\neq i}^{n}|a_{ji}|x_j$ ，$i=1,2,\cdots,n$ ，则 $r^x=(r_1^x,r_2^x,\cdots,r_n^x)$ 和 $c^x=(c_1^x,c_2^x,\cdots,c_n^x)$ 也是 G−函数 [6] .

**定义 2**　设 $\boldsymbol{A}$ 为 $n$ 阶方阵，若存在 G−函数 $f=(f_1,f_2,\cdots,f_n)$ ，使得

$$|a_{ii}|>f_i(\boldsymbol{A}),\qquad i=1,2,\cdots,n \tag{1}$$

则称 $\boldsymbol{A}$ 为严格 G−对角占优的矩阵.

元素都是非负实数的矩阵称为非负矩阵，因而从矩阵论的角度看，一幅灰度图像可以看成是一个非负矩阵. 将由灰度图像 (长和宽相等) 得到的矩阵记为 $\boldsymbol{B}$ ，则 $\boldsymbol{B}$ 是一个 $n$ 阶非负矩阵. 一般来说，矩阵 $\boldsymbol{B}$ 并不是严格 G−对角占优的，为此我们令

$$\boldsymbol{A}=s\boldsymbol{I}-\boldsymbol{B},\qquad s>0 \tag{2}$$

则我们有下面的定理.

**定理 1**　设 $\boldsymbol{A}$ 为具有形如式 (2) 的 $n$ 阶方阵，$\rho(\boldsymbol{B})$ 为矩阵 $\boldsymbol{B}$ 的谱半径，若 $s>\rho(\boldsymbol{B})$ ，则矩阵 $\boldsymbol{A}$ 是严格 G−对角占优的，且 $|\boldsymbol{A}|>0$ .

证明见参考文献 [7] .

所谓矩阵的 LU 分解是指：对任何一个方阵 $\boldsymbol{A}$ 可以表示成一个下三角矩阵 $\boldsymbol{L}$ 和一个上三角矩阵 $\boldsymbol{U}$ 的乘积：$\boldsymbol{A}=\boldsymbol{LU}$ ，其中矩阵 $\boldsymbol{L}$ 的对角线元素全为 1 .

设 $\boldsymbol{A}$ 为形如式 (2) 的矩阵，若 $\boldsymbol{A}$ 为 G−对角占优的，则存在 G−函数 $f=(f_1,f_2,\cdots,f_n)$ ，使得式 (1) 成立，且 $|\boldsymbol{A}|>0$ ，由于 $\boldsymbol{A}$ 的任意主子阵也具有式 (2) 的形式且是 G−对角占优的，因而矩阵 $\boldsymbol{A}$ 的任意主子式为正数. 由矩阵三角分解定理可得下面的结论.

**定理 2**　设 $\boldsymbol{A}$ 为形如式 (2) 的矩阵，若 $\boldsymbol{A}$ 为 G−对角占优的，则存在下三角矩阵 $\boldsymbol{L}$ 和一个上三角矩阵 $\boldsymbol{U}$ 使得 $\boldsymbol{A}=\boldsymbol{LU}$ ，这里矩阵 $\boldsymbol{L}$ 的对角线的元素全为 1 ，矩阵 $\boldsymbol{U}$ 的对角线上的元素全为正数.

这样，对于给定的一幅灰度图像，就可以得到一个非负矩阵 $\boldsymbol{B}$ ，选取适当的 $s$(可作为密钥进行保存用以提高嵌入水印的安全性) ，使得矩阵 $\boldsymbol{A}=s\boldsymbol{I}-\boldsymbol{B}$ 为 G−对角占优的，再对矩阵 $\boldsymbol{A}$ 进行 LU 分解，则可使得矩阵 $\boldsymbol{L}$ 的对角线的元素全为 1 ，矩阵 $\boldsymbol{U}$ 的对角线上的元素全为正数.

下面我们利用上面的结论给出数字水印的嵌入算法.

## 3 基于 LU 分解的数字水印嵌入方法

为了提高水印的嵌入量，同时也为了与基于 DCT 变换的嵌入方法进行比较，我们首先将原始图像进行 $8\times 8$ 的分块. 记矩阵 $\boldsymbol{B}$ 为其中的任意的一块，则 $\boldsymbol{B}$ 为 $8\times 8$ 的非负矩阵. 令 $\boldsymbol{A}=s\boldsymbol{I}-\boldsymbol{B}$，选取 $s$，使得 $s>\rho(\boldsymbol{B})$，则矩阵 $\boldsymbol{A}$ 是严格 G-对角占优的. 对矩阵 $\boldsymbol{A}$ 进行 LU 分解 $\boldsymbol{A}=\boldsymbol{LU}$，则下三角矩阵 $\boldsymbol{L}$ 的对角线元素全为 1，上三角矩阵 $\boldsymbol{U}$ 的对角线元素全为正数.

对于水印图案 $W$ 将其转化为一维向量，记为 $\boldsymbol{W}$. 对于给定的步长 $a$，对 LU 分解后的矩阵 $\boldsymbol{U}$ 的对角线元素进行量化，具体做法为：当 $\boldsymbol{W}(i)=0$ 时，修改矩阵 $\boldsymbol{U}$ 的对角线元素 $u_{ii}$ 的值，使得 $u_{ii}$ 等于与 $u_{ii}$ 距离最近的 $a$ 的偶倍数的值；当 $\boldsymbol{W}(i)=1$ 时，修改元素 $u_{ii}$ 的值，使得 $u_{ii}$ 等于与 $u_{ii}$ 距离最近的 $a$ 的奇倍数的值；将修改后的矩阵记作 $\boldsymbol{U}'$，令 $\boldsymbol{A}'=\boldsymbol{LU}'$，再令 $\boldsymbol{B}'=s\boldsymbol{I}-\boldsymbol{A}'$，将 $\boldsymbol{B}'$ 作为含水印的图像数据，重建图像.

水印的提取为上述过程的逆过程，根据对矩阵 $\boldsymbol{A}'$ 进行 LU 分解后的矩阵 $\boldsymbol{U}$ 的对角线元素 $u_{ii}$ 靠近步长 $a$ 的偶数倍还是奇数倍来决定提取出的数据是 0 还是 1，由此得到一维向量 $\boldsymbol{W}^*$，根据 $\boldsymbol{W}^*$ 重建水印图案.

为了对提取出的水印图像质量给出一个客观的评价标准，我们采用恢复水印 $\boldsymbol{W}^*$ 与嵌入水印的归一化相关值作为一种客观的衡量标准，其公式定义如下：

$$\mathrm{NC}=\sum_i \boldsymbol{W}^*(i)\cdot\boldsymbol{W}(i)\Big/\sum_i \boldsymbol{W}(i)^2 \tag{3}$$

在进行水印的嵌入过程中，我们没有对矩阵 $\boldsymbol{B}$ 直接进行 LU 分解，这主要是由于矩阵 $\boldsymbol{B}$ 可能是奇异的，因而分解后的矩阵 $\boldsymbol{U}$ 的对角线元素会出现 0，按邻近值算法修改后，对原图影响较大；再有对矩阵 $\boldsymbol{B}$ 直接进行分解后矩阵 $\boldsymbol{U}$ 的对角线元素的值太小，给步长 $a$ 的确定带来困难，又由于计算的误差，使得提取效果非常差.

## 4 实验结果及分析

本文算法全部在 Matlab 6.1 平台上得以实现，下面是对算法仿真的一些结果.

我们对几幅不同的图像进行了实验，但限于篇幅，仅以 Lena 256 图像作为例子. 实验中，将原始图像按 8×8 进行分块，共有 1024 个小块. 记矩阵 $\boldsymbol{B}_i(i=1,2,\cdots,1024)$ 为其中的任意一块，取正数序列 $\{k_1,k_2,\cdots,k_{1024}\}$ 作为密钥进行保存，令 $s_i=k_i+\rho(\boldsymbol{B}_i)$，则 $\boldsymbol{A}_i=s_i\boldsymbol{I}-\boldsymbol{B}_i$ 是 G-对角占优矩阵，参照 JPEG 压缩中的量化矩阵，选取步长 $a=16$.

为了说明这种算法具有很好的鲁棒性，我们将这种方法与 DCT 域上的中频系数比较法进行了对比 [8]. 所谓 DCT 中频系数比较法，就是将原始图像同样按 8×8 进行分块，将 DCT 的中频系数进行适当分组，按照每 3 个一组，分为 8 组，通过改变每组中 3 个数的次序来表达水印信息，由于 DCT 的中频系数值相对都比较接近，为增加水印的强度，需要选择适当的参数 $d$，通过参数 $d$ 来调节嵌入水印的强度. 即当每组 3 个数中最大的数与最小的数相差小于参数 $d$ 时，人为增大它们之间的差距使之大于参数 $d$，这里取 $d=2$. 由于 DCT 的中频系数一般比较小，实验结果显示用 DCT 中频系数比较法比用 DCT 中频系数直接量化的效果要好，虽然可以在 DCT 的低频系数上通过量化的方法嵌入数字水印，但对图像的质量影响较大，这是由于人眼对 DCT 的低频分量敏感，而对中频系数的修改不会使图像出现明显的降质.

下面的图像中图 1 为原始图像，图像的尺寸为 256×256，图 2 为原始图像使用基于矩阵 LU 分解方法嵌入水印后的图像，尺寸不变，图 3 为原始水印，尺寸为 $90\times 80$.

图 1　原始图像

图 2　嵌入水印后图像


图 3　原始水印

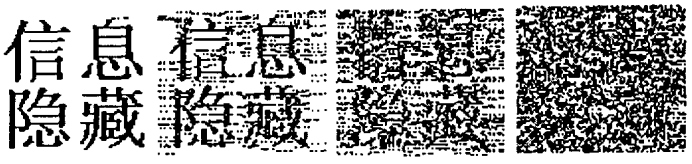
为验证使用该算法嵌入到图像中的水印信息的抵抗攻击能力．实验中对嵌入水印的图像进行攻击，然后提取水印图案，限于篇幅，仅就下面两种攻击进行说明．

**4.1 JPEG 压缩处理**

下面的图像中，图 4 为用 LU 算法嵌入水印后的图像选取不同的质量因子经 JPEG 压缩处理后得到的图像， Quality 的值如图中所示，图 5 为 DCT 中频系数比较法 (图像略去) 按图 4 中的 Quality 值经 JPEG 压缩处理后，依次从中提取的水印图案．图 6 为从图 4 中依次提取的水印图案．

(a) Quality=97%　(b) Quality=95%　(c) Quality=90%　(d) Quality=85%

图 4　含水印图像经 JPEG 压缩处理后得到的图像




(a) NC=0.9986 (b) NC=0.8670 (c) NC=0.6589 (d) NC=0.4716

图 5　DCT 中频系数比较法在不同的 Quality 值下提取的水印图案


(a) NC=0.9972　(b) NC=0.9948　(c) NC=0.9756　(d) NC=0.9064

图 6　LU 算法在不同的 Quality 值下提取的水印图案

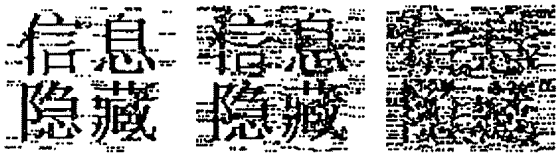
从上面的水印可以看出：与 DCT 中频系数比较法相比， LU 算法的抗 JPEG 压缩的性能要好，并且当加大攻击强度时，用 DCT 中频系数比较法提取的水印其清晰度下降很快，用 LU 算法提取的水印的清晰度下降缓慢，因而 LU 算法对 JPEG 压缩具有很好的鲁棒性.

**4.2 高斯噪声处理**

下面的图像中给出了在 3 种不同方差下的对比实验. 图 7 为用 LU 算法嵌入水印后的图像经选取不同的方差添加高斯噪声后得到的图像，方差 $\sigma^2$ 的值如图中所示. 图 8 为用 DCT 中频系数比较法按图 7 中的 $\sigma^2$ 的值添加高斯噪声后，依次提取的水印图案. 图 9 为从图 7 中依次提取的水印图案.

(a) $\sigma^2$=0.0005 (b) $\sigma^2$=0.0001 (c) $\sigma^2$=0.0002

图 7 含水印的图像添加高斯噪声后得到的图像



(a) NC=0.9485 (b) NC=0.8301 (c) NC=0.6870

图 8 DCT 中频系数比较法在不同方差下提取的水印

(a) NC=0.9925 (b) NC=0.9712 (c) NC=0.9310

图 9 LU 算法在不同方差下提取的水印

由以上图像的对比可以看出，对于添加高斯噪声， DCT 中频系数比较法提取的水印比 LU 算法要差. 对于 DCT 中频系数比较法，当加大攻击强度，即加大高斯噪声时，提取水印的清晰度下降很快，而 LU 算法，水印的清晰度下降要慢的多，因此可以得出 LU 算法的抗高斯噪声的性能比 DCT 中频系数比较法好. LU 算法对经过高斯噪声处理的图像具有很好的鲁棒性.

为进一步说明 LU 算法的鲁棒性，我们还与 Cox 的扩展谱方法 [4,9] 做了对比实验，实验结果显示两者的鲁棒性基本一致，限于篇幅，不再赘述，但 LU 算法的运算速度要快得多. 在实验中，我们使用主频为 450MHz 的计算机，使用 Cox 的嵌入方法大约需要 1 个小时，而使用 LU 算法则只需要 2 分钟左右，这是由于 LU 分解实际上就是线性方程组中的 Gauss 消去法，其运算速度比 DCT 变换要快的多.

## 5 结论

本文提出了一种新的数字水印算法，水印被叠加到原始图像的 LU 域上．该算法利用了矩阵理论中 G-对角占优矩阵的 LU 分解，数学背景清晰．实验结果表明：新算法不仅运算速度快，而且比 DCT 中频系数比较法要鲁棒的多．对于抗 JEPG 压缩和高斯噪声， LU 算法比 DCT 中频系数比较法有更好的性能，当攻击的强度逐渐加大时，水印图案的清晰程度不会出现急速下降，因而对于在静态图像中嵌入水印， LU 方法是一项有着发展前途的数字水印嵌入算法．

## 参 考 文 献


[1] Van Schyndel R G, Tirkel A Z, Osborne C F. A digital watermark[A]. Proc. IEEE Int'l Conference on Image Processing[C]. IEEE CS Press, Los Alamitos, California, USA, 1994, 2: 86–90.

[2] Wolfgang R B, Delp E G. A watermark for digital image[A]. Proc. IEEE Int'l Conference on Image Processing[C]. IEEE CS Press, Los Alamitos, California, USA, 1996, 3: 219–222.

[3] Cox I J, Linnartz J P M G. Some general methods for tampering with watermarks[J]. *IEEE J. on Selected Areas in Communications*, 1998, 16(4): 587–593.

[4] Cox I J, Kilian J, Leighton F T, Shamoon T. Secure spread spectrum watermarking for multimedia[J]. *IEEE Trans. on Image Processing*, 1997, 6(12): 1673–1687.

[5] 钮心忻，杨义先．基于小波变换的数字水印隐藏与检测算法 [J]．计算机学报， 2000, 23(1): 21–27.

[6] 牛少彰，关于一类复方阵的 LU 分解 [J]．北京邮电大学学报， 1995, 18(2): 64–67.

[7] 陈公宁．矩阵理论与应用 [M]．北京：高等教育出版社， 1990: 319–324.

[8] 牛少彰，钮心忻，杨义先，陈宇丰．基于密钥分存原理的数字水印分存技术 [A]，信息隐藏全国学术研讨会 (CIHW20002) 论文集 [C]．北京：机械工业出版社，大连， 2002 年 8 月： 145–151.

[9] 刘瑞祯，谭铁牛．基于奇异值分解的数字图像水印方法 [J]．电子学报， 2001, 29(2): 168–171.



牛少彰：　男， 1963 年生，教授，主要研究领域为图象处理、信息隐藏、数字水印、网络信息安全和应用数学．

钮心忻：　男， 1963 年生，副教授，博士，主要研究领域为信息安全、信号信息处理、信息隐藏和数字水印．

杨义先：　男， 1961 年生，教授，博士生导师， 1999 年 3 月至今，被聘为长江学者奖励计划特聘教授．主要研究领域为密码学、网络信息安全、信号与信息处理．已发表论文 300 余篇，出版专著 7 本．