

基于 Hadamard 变换和 LU 分解的盲水印算法

吴 捷¹, 马小虎²

(1. 泰州职业技术学院 信息工程学院, 江苏 泰州 225300;

2. 苏州大学 计算机科学与技术学院, 江苏 苏州 215006)

摘 要:为提高传统数字图像水印算法的安全性,解决数字水印对信号处理和几何失真比较敏感的问题,提出一种基于 Hadamard 变换和 LU 分解的盲水印嵌入算法。不同于常见的变换域数字水印技术,该方案对原始图像进行二维 Hadamard 变换(HT),将得到的变换图像进行 8×8 分块,然后对每个分块进行 LU 及 SVD 分解,从得到的对角矩阵中选择一个关键位嵌入水印。通过计算所有关键位的平均值,并比较每个关键位和平均值的大小关系,计算得到密钥,利用密钥实现了水印的盲检测。实验结果表明,提出的盲水印算法不但具有较好的保真度,对于各种攻击也具有较强的鲁棒性。

关键词:数字水印;Hadamard 变换;LU 分解;鲁棒性

中图分类号:TP391.41

文献标识码:A

文章编号:1673-629X(2016)02-0082-05

doi:10.3969/j.issn.1673-629X.2016.02.019

A Blind Digital Image Watermarking Algorithm Based on Hadamard Transform and LU Decomposition

WU Jie¹, MA Xiao-hu²

(1. School of Information Engineering, Taizhou Polytechnic College, Taizhou 225300, China;

2. School of Computer Science and Technology, Soochow University, Suzhou 215006, China)

Abstract:In order to improve the security of traditional digital image watermarking algorithm and solve the problem of digital watermark is sensitive to signal processing and geometric distortion, a new digital watermarking algorithm based on LU decomposition and Hadamard transform was proposed. Unlike the common transform domain watermarking techniques, this scheme decomposes the whole image with two-dimensional Hadamard transform firstly, and then divides the image into 8×8 blocks, taking LU and SVD decomposition for each block, selecting an embedded position of each block to add watermarking. By calculating the average of all the embedded position value, and comparing each embedded position value with average value, get the key which is used to realize the blind detection. Experimental results show the blind watermarking algorithm proposed not only has good fidelity, but also owns great robustness to various attacks.

Key words:digital watermarking;Hadamard Transforms (HT);LU decomposition;robustness

1 概 述

数字水印技术在近几年得到了广泛的重视。它通过在原始数据中嵌入秘密信息(水印)来证实该作品的所有权。数字水印技术从不同的角度可以有不同的分类。按水印的嵌入方法可以分为空域水印技术和变换域水印技术;按检测水印方法可以分为非盲水印算法和盲水印算法。

空域水印算法主要是通过修改原始图像的像素实现的,变换域水印算法则是通过运用适当的算法修改变换系数实现的。空域水印算法非常简单有效,但是

水印的鲁棒性较差,无法经受一些常见的攻击。而变换域^[1-6]技术在解决了嵌入强度问题的同时还保证了水印的不可感知性,具有较高的隐蔽性和安全性,近几年的众多研究成果大多是基于变换域展开的。其中文献[1]结合小波变换和 SVD 提出了一种多水印算法,首先对整个图像应用三级离散小波变换,然后在低频和中频区域分别嵌入水印,最后由提取出的三份水印生成第四份水印作为最终检测水印。文献[2]中算法先对载体图像进行 n 层的离散小波变换,然后随机选取其中的部分或全部子带形成参考子带并进行 SVD 分解,最后将置乱处理后的水印嵌入奇异值矩阵中。

收稿日期:2015-05-12

修回日期:2015-08-13

网络出版时间:2016-01-26

基金项目:江苏省自然科学基金项目(BK20141195)

作者简介:吴 捷(1982-),男,讲师,硕士,研究方向为数字图像处理;马小虎,教授,博士,硕导,研究方向为数字图像处理、模式识别等。

网络出版地址:<http://www.cnki.net/kcms/detail/61.1450.TP.20160126.1520.038.html>

文献[3]提出了一种基于奇异值变换和小波包分解的自适应鲁棒水印算法。首先将原始图像进行 8×8 分块,并对每一子块进行小波包分解。根据人眼视觉特性和图像块自身的亮度以及纹理特征确定最佳量化步长,将水印信息通过量化调制的方法自适应地嵌入至相应高低频区域的奇异值中。文献[1-3]代表的这一类算法在提取水印时都需要原始图像和水印的参与,属于非盲水印算法。非盲水印算法的鲁棒性较强,但其应用受到存储成本的限制。因此,近年来盲水印算法受到越来越多的关注。

文献[7]提出了一种基于人类视觉特性的小波域盲数字水印算法,具有一定的抗噪声、JPEG 压缩和滤波等攻击能力,能够较好地达到水印嵌入透明性和鲁棒性的平衡。文献[8]提出了一种改进的基于 DCT 的自适应盲数字水印。DCT 块的 DC 分量利用奇偶量化法嵌入水印,AC 分量利用确定固定系数法嵌入水印,实现了水印的盲检测。文献[9]根据压缩感知(Compressive Sensing, CS)的特点,结合人眼视觉系统(HVS)的特性,提出一种性能更高的数字水印算法,利用块不均匀度来选取容量大的子块,采用量化的方法自适应地选择量化步长来嵌入经过置乱处理后的数字水印。

文中的主要贡献在于,结合 Hadamard 变换和 LU 分解技术提出一种新的盲水印算法。和已有算法相比,该算法加入水印后对原始图像的影响较小,并且具有较强的鲁棒性。

2 图像的 Hadamard 变换

Hadamard 变换(又称沃尔什-哈达玛变换,沃尔什变换或者沃尔什-傅里叶变换)是一种广义傅里叶变换。哈达玛(Hadamard)变换本质上是一种特殊排序的沃尔什变换,Hadamard 矩阵 H_m 代表了一个 $M \times M$ 的矩阵,其中 $M = 2^m, m = 1, 2, \dots$ 。 H_m 矩阵的值为 1 或 -1, H_m 的行和列是正交的。对于变换域水印算法,时频变换过程在整个水印算法中占主要部分。水印算法中常用的一些变换操作,如 DFT 和 DCT 变换等,都要用到复数乘法,水印嵌入过程通常会耗时较多。Hadamard 变换过程存储空间小,运算速度快,在图像处理和图像压缩领域已经得到广泛应用。而在数字水印领域,国内外的相关文献并不多,只有文献[10-12]在这一领域进行了相关研究。二维 Hadamard 矩阵如式(1)所示:

$$H_m = \begin{bmatrix} H_{m-1} & H_{m-1} \\ H_{m-1} & -H_{m-1} \end{bmatrix} \quad (1)$$

其中, $m > 0$, 当 $m = 1$ 时, $M = 2$, 因此 2×2 的 Had-

amard 矩阵如下:

$$H = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad (2)$$

设 O 代表原始图像, T 代表变换后的图像,二维 Hadamard 变换公式表示如下:

$$[T] = \frac{H_m [O] H_m}{M} \quad (3)$$

由式(3)可以推算出二维 Hadamard 变换的逆变换,公式表示如下:

$$[O] = H_m^{-1} [T] H_m^* = \frac{H_m [T] H_m}{M} \quad (4)$$

3 矩阵的 LU 分解

对于任意 n 阶方阵 F ,若有下三角阵 L 和上三角阵 U ,使得 $F = LU$,则称 A 可以三角分解,称 $F = LU$ 为 F 的 LU 分解。LU 分解如式(5):

$$F = L \times U = \begin{bmatrix} 1 & 0 & 0 \\ l_{21} & 1 & 0 \\ l_{31} & l_{32} & 1 \end{bmatrix} \times \begin{bmatrix} d_1 & u_{12} & u_{13} \\ 0 & d_2 & u_{23} \\ 0 & 0 & d_3 \end{bmatrix} \quad (5)$$

文中算法对 LU 分解进行了变换,将矩阵 U 进行进一步分解得到了由系数 d_n 构成的对角矩阵 D ,使 LU 分解变为 LDU 分解。变换后的公式和基本实现程序如下:

$$F = L \times D \times U = \begin{bmatrix} 1 & 0 & 0 \\ l_{21} & 1 & 0 \\ l_{31} & l_{32} & 1 \end{bmatrix} \times \begin{bmatrix} d_1 & 0 & 0 \\ 0 & d_2 & 0 \\ 0 & 0 & d_3 \end{bmatrix} \times \begin{bmatrix} 1 & \frac{u_{12}}{d_1} & \frac{u_{13}}{d_1} \\ 0 & 1 & \frac{u_{23}}{d_2} \\ 0 & 0 & 1 \end{bmatrix} \quad (6)$$

```
function [ L,D,U ] =LDU( A )
[ L,U ] =lu( A );
b = size( A );
n = b( 1 );
D = zeros( n,n );
for i = 1 : n
D( i , i ) = U( i , i );
end
U = inv( D ) * U ;
```

国内外关于 LU 分解在数字水印领域应用的研究比较少^[13-14]。和 SVD 一样,在 LDU 分解中对角矩阵 D 系数的修改对原始图像的视觉影响很小。文中的研究工作拓展了数字水印的应用领域,将 Hadamard 算法和 SVD、LDU 等技术结合到一起设计了一种新的水印算法,既保证算法实现的快速性,又能显著减少加入水印对原始图像的视觉影响。

4 水印的嵌入与提取

4.1 水印的嵌入

文中所提算法是先将原始图像进行 Hadamard 变换和 LU 分解,然后利用乘性准则将水印嵌入到子块中。原始图像选择 256 灰度等级($N \times N$)的标准图像 I ,二值水印图像大小为 $\frac{N}{8} \times \frac{N}{8}$ 。

- 其步骤可总结如下:
- (1)对 I 进行 Hadamard 变换(HT),得到变换后的图像 I' 。
- (2)对 I' 进行 8×8 分块,得到 $\frac{N}{8} \times \frac{N}{8}$ 个分块,对每个分块进行 LU 分解: $F = L \times D \times U$, 再对矩阵 D 进行 SVD 分解: $[U, S, V] = \text{svd}(D)$, 从每个分块的 S 矩阵中选择一位作为嵌入位,记为 S_n ($n = 1, 2, \dots, \frac{N}{8} \times \frac{N}{8}$)。文中算法选择 $[1, 1]$ 位为嵌入位。

- (3)运用乘性准则嵌入水印:
- $$S_n = S_n * (1 + \alpha w(i, j)) \quad (i = 1, 2, \dots, \frac{N}{8}, j = 1, 2, \dots, \frac{N}{8})$$
- 其中, α 为嵌入强度因子; $w(i, j)$ 为水印值。

- (4)利用公式 $T = \frac{1}{M} \sum_{n=1}^M S_n$, 计算嵌入水印后所有嵌入位数值的平均值,其中 $M = \frac{N}{8} \times \frac{N}{8}$ 。
- (5)根据式(1)比较每个嵌入位数值和平均值的大小关系,数值存入 $c(m, 1)$ ($m = 1, 2, \dots, \frac{N}{8} \times \frac{N}{8}$)。

- $$\begin{aligned} c(m, 1) &= 1 && \text{if } S_n \geq T \\ c(m, 1) &= 0 && \text{if } S_n < T \end{aligned} \tag{1}$$
- (6)利用步骤(4)得到的 $c(m, 1)$ 和 $w(i, j)$ 进行异或操作:
- $$k(i, j) = c(m, 1) \text{ XOR } w(i, j)$$
- 得到提取水印密钥 $k(i, j)$ 。

4.2 水印的提取

- 水印提取是水印嵌入的逆过程,具体步骤如下:
- (1)对待测图像 I^* 进行 Hadamard 变换,得到变换后的图像 $I^{*'}$ 。
- (2)对 $I^{*'}$ 进行 8×8 分块,得到 $\frac{N}{8} \times \frac{N}{8}$ 个分块,对每个分块进行 LU 分解: $F = L \times D \times U$, 再对矩阵 D 进行 SVD 分解: $[U, S, V] = \text{svd}(D)$, 计算所有 S 矩阵中 $[1, 1]$ 位数值(记为 S'_n)的平均值(记为 T')。
- (3)根据式(2)比较 S'_n 和平均值的大小关系,得到 $c'(m, 1)$ 。

- $$\begin{aligned} c'(m, 1) &= 1 && \text{if } S'_n \geq T' \\ c'(m, 1) &= 0 && \text{if } S'_n < T' \end{aligned} \tag{2}$$
- (4)用 $c'(m, 1)$ 和 $k(i, j)$ 进行异或操作:
- $$g(i, j) = c'(i, 1) \text{ XOR } k(i, j)$$
- 得到提取出的水印 $g(i, j)$ 。

5 实验结果与分析

文中实验采用 Matlab7.0 进行仿真,原始图像采用 512×512 像素的 Lena、Boat、Peppers、Baboon 标准灰度图像,水印图像采用 64×64 像素的“苏州大学”字的二值图像。对图像质量的评价标准采用峰值信噪比 PSNR,水印检测结果的评价标准采用提取出来的水印 W^* 和原始水印 W 之间的相似度 NC 进行衡量。

表 1 是未经任何攻击提取出的水印参数,NC 依次为 0.998 5、0.999 1、0.999 7、0.998 5,都没有达到 1,但偏差很小,影响不大,因此可以忽略。PSNR 值依次为 47.574 6、46.189 6、48.541 5、47.520 2,因此文中算法嵌入的水印信息对原始图像影响很小,并且可以正确提取。

表 1 未受攻击下的 NC 和 PSNR 值

原始图像	NC	PSNR/dB
Lena	0.998 5	47.574 6
Boat	0.999 1	46.189 6
Peppers	0.999 7	48.541 5
Baboon	0.998 5	47.520 2

表 2 中给出了四幅加水印后的测试图像经受各种类型攻击的详细参数。图 1 是 4 幅测试图像经受各种攻击的参数。

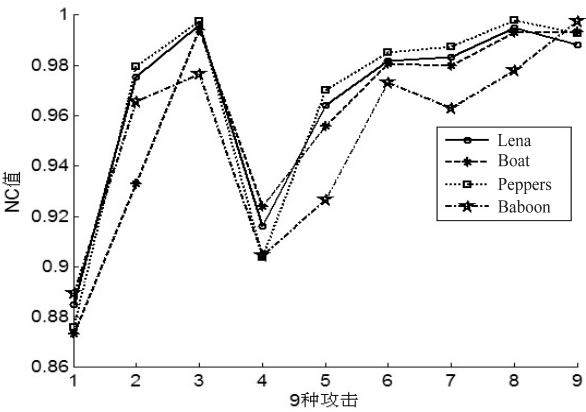


图 1 各种测试图像攻击结果比较

从中可以看出,对于不同的测试图片,文中算法的结果基本都稳定在 0.9 以上,说明了该算法的有效性和通用性。图 2(a)给出了原始图像和原始水印,图 2(b)–(h)则给出部分攻击后采用文中的盲检测算法提取出的水印,可以看出提取出的水印辨识度较高。

表 3、表 4 是文中算法和文献[3,7]算法的比较。

表 2 不同水印图像攻击测试结果

攻击方式	Lena		Boat		Peppers		Baboon	
	PSNR	NC	PSNR	NC	PSNR	NC	PSNR	NC
旋转 15°	11.534 7	0.884 9	11.331 0	0.873 3	10.493 9	0.876 0	12.166 6	0.889 3
直方图均衡化攻击	19.159 5	0.975 5	17.373 3	0.932 9	18.565 7	0.979 6	17.582 3	0.965 5
中值滤波[3 3]	35.106 7	0.996 2	31.894 5	0.994 2	34.811 7	0.997 4	23.724 1	0.976 7
裁剪(20:276,20:276)	11.516 4	0.916 2	14.920 0	0.924 0	9.632 0	0.903 7	11.173 0	0.904 3
高斯噪声[0 0.02]	17.176 4	0.964 2	17.270 7	0.955 9	17.402 3	0.970 0	17.113 8	0.926 6
JPEG10% 压缩比	30.278 7	0.981 8	28.746 8	0.980 7	30.094 8	0.985 3	23.399 5	0.973 0
椒盐噪声(0.02)	22.352 6	0.983 2	22.337 6	0.980 1	22.176 1	0.987 4	22.510 5	0.963 2
高斯低通滤波[3 1]	33.249 8	0.995 1	31.023 6	0.993 0	32.875 2	0.998 0	24.577 9	0.978 0
图像增强[0,0.8],[0,1]	17.493 7	0.988 1	16.535 0	0.993 5	18.407 4	0.992 7	17.114 1	0.997 6

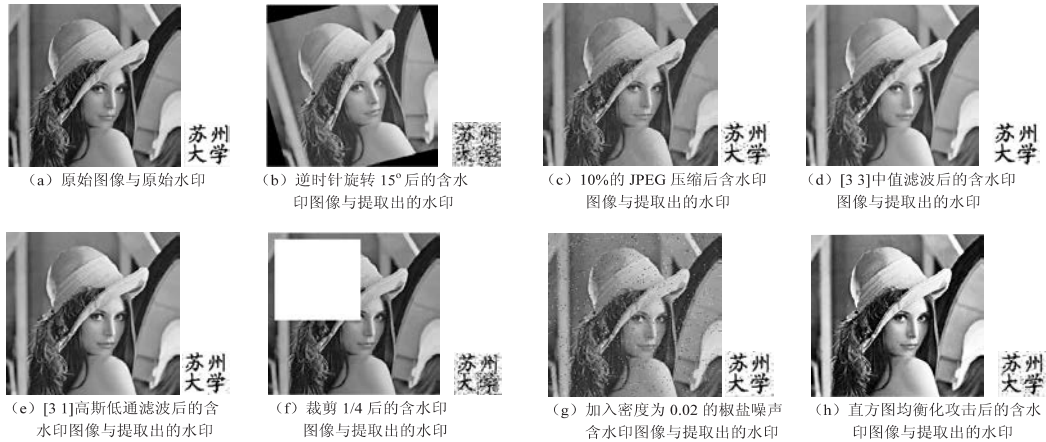


图 2 Lena 图像测试结果

文献[3]的测试载体图像使用的是 512×512 的 Lena 图像,水印使用的是 32×32 的二值图像“南京大学”,加入水印后图像的 PSNR 值分别为 47.247。文中构造了 64×64 的二值图像“南京大学”水印进行测试,文中算法加入水印后图像的 PSNR 值为 47.822 4,略高于文献[3]。从表 3 的比较可以看出,除了旋转图像外,文中算法在各种攻击下的表现要优于文献[3]。

文献[7]的测试载体图像使用的是 512×512 的 Lena 图像,水印使用的是 64×64 的二值图像“浙江大学”,加入水印后图像的 PSNR 值为 47.619 3。文中构造了和文献[7]完全相同的水印进行测试,文中算法加入水印后图像的 PSNR 值为 47.873 7。从表 4 的比

较可以看出,文中算法在各种攻击下的表现都要优于文献[7]。

6 结束语

文中基于 Hadamard 变换和 LU 分解,提出了一种新的数字水印算法。和之前算法不同的是,文中首先对载体图像进行 Hadamard 变换,将得到的图像再进行 8*8 分块,并对每一分块进行 LU 分解和 SVD 分解,然后从每个分块中选择一个嵌入位完成水印的嵌入。后续操作则通过计算所有嵌入位的平均值,并比较每个嵌入位和平均值的大小关系,进而得到密钥,利用密钥实现了水印的盲检测。和已有算法相比,文中提出

表 3 文中算法与文献[3]算法的比较

攻击类型	文中算法	文献[3]算法
JPEG 压缩(75% 压缩比)	0.997 7	0.993 2
JPEG 压缩(30% 压缩比)	0.992 2	0.930 1
高斯噪声(0.004)	0.986 4	0.941 4
中值滤波(3×3)	0.996 2	0.941 8
高斯滤波(3×3)	0.995 1	0.954 6
几何旋转(10°)	0.895 7	0.957 8

表 4 文中算法与文献[7]算法的比较

攻击类型	文中算法	文献[7]算法
JPEG 压缩(60% 压缩比)	0.997 0	0.990 7
JPEG 压缩(40% 压缩比)	0.994 5	0.941 6
JPEG 压缩(20% 压缩比)	0.991 8	0.806 2
高斯噪声(0.004)	0.986 4	0.817 7
椒盐噪声(0.01)	0.989 3	0.932 0
中值滤波(3×3)	0.996 2	0.945 7

的盲水印算法不但具有较好的保真度,对于各种攻击也具有较强的鲁棒性。

将来的主要工作在于研究嵌入位的不同选择对于实验结果的影响,以找到更加有效的方法来实现水印的嵌入。

参考文献:

[1] 薛胜男,陈秀宏. 基于混沌加密和 SVD 的数字图像水印算法[J]. 计算机工程,2012,38(19):107-110.

[2] 熊祥光,王 力. 一种改进的 DWT-SVD 域参考水印方案[J]. 计算机工程与应用,2014,50(7):75-79.

[3] 朱 光,张军亮. 基于 SVD 和小波包分解的自适应鲁棒水印算法[J]. 计算机应用研究,2013,30(4):1230-1233.

[4] 雷 蕾,郭树旭,王 雷. 基于小波变换的 SVD 数字图像水印算法研究[J]. 计算机仿真,2013,30(9):169-172.

[5] 陈 军,张 伟,杨华千,等. 一种基于小波变换和神经网络的数字水印算法[J]. 计算机科学,2011,38(6):142-144.

[6] 张秋余,李 凯,袁占亨. 基于混沌和 SVD-DWT 的稳健数字图像水印算法[J]. 计算机应用研究,2010,27(2):718-720.

[7] 叶 闯,沈益青,李 豪,等. 基于人类视觉特性(HVS)的

离散小波变换(DWT)数字水印算法[J]. 浙江大学学报:理学版,2013,40(2):152-155.

[8] 季 燕. 基于 DCT 的自适应盲数字水印[J]. 计算机科学,2013,40(7):129-130.

[9] 廖 斌,任美玲,徐俊刚. 一种基于压缩感知的盲数字水印算法[J]. 计算机应用与软件,2014,31(2):307-311.

[10] Ho A T S,Shen J,Chow A K K,et al. Robust digital image-in-image watermarking algorithm using the fast Hadamard transform[C]//Proceedings of the international symposium on circuit and system 2003. [s. l.]:IEEE,2003:826-829.

[11] Saryazdi S,Nezamabadi-Pour H. A blind digital watermark in Hadamard domain[C]//Proceedings of world academy of science,engineering and technology. [s. l.]:[s. n.],2005:498-502.

[12] 李红丽,赖惠成. 基于哈达玛变换和奇异分解的四个彩色图像水印算法[J]. 计算机应用,2010,30(11):3025-3027.

[13] Niu Shaozhang,Niu Xinxin,Yang Yixian. Digital watermarking algorithm based on LU decomposition[J]. Journal of Electronics &Information Technology,2005,26(10):1620-1625.

[14] 王树梅,赵卫东,王志成. 一种基于 LU 的小波域自适应数字水印算法[J]. 微电子学与计算机,2008,25(12):76-79.

(上接第 81 页)

器网络密钥管理方案[J]. 电子学报,2013,41(2):214-219.

[7] Duarte-Meloe J,Liu M Y. Analysis of energy consumption and lifetime of heterogeneous wireless sensor networks[C]//Proceedings of IEEE GLOBEC-OM. Taipei:IEEE,2002:21-25.

[8] 马春光,尚治国,王慧强. 基于区域的异构无线传感器网络密钥管理[J]. 通信学报,2009,30(5):74-81.

[9] 马春光,张秉政,孙 原,等. 基于按对平衡设计的异构无线传感器网络密钥预分配方案[J]. 通信学报,2010,31(1):37-43.

[10] Heinzelman W,Chandrakasan A,Balakrishan H. An application-specific protocol architecture for wireless microsensor networks[J]. IEEE Transactions on Wireless Communications,2002,1(4):660-670.

[11] Younis O,Fahrmy S. Heed:a hybird,energy-efficient,distributed clustering approach for ad-hoc sensor networks[J]. IEEE Trans on Mobile Computing,2004,3(4):660-669.

[12] 李成法,陈贵海,叶 懋,等. 一种基于非均匀分簇的无线传感器网络路由协议[J]. 计算机学报,2007,30(1):27-36.

[13] Qing Li,Zhu Qingxin,Wang Mingwen. A distributed energy-efficient clustering algorithm for heterogeneous wireless sensor networks[J]. Journal of Software,2006,17(3):1282-1291.


[14] 刘 唐,孙彦清. 基于负载均衡和最短路径的异构无线传感器网络成簇算法[J]. 计算机科学,2014,41(10):169-172.

[15] 刘 唐,汪小芬,杨 进. 基于相对距离的多级能量异构传感器网络成簇算法[J]. 计算机科学,2012,39(8):119-121.

基于Hadamard变换和LU分解的盲水印算法

作者：[吴捷](#)，[马小虎](#)，[WU Jie](#)，[MA Xiao-hu](#)

作者单位：[吴捷, WU Jie\(泰州职业技术学院 信息工程学院, 江苏 泰州, 225300\)](#)，[马小虎, MA Xiao-hu\(苏州大学 计算机科学与技术学院, 江苏 苏州, 215006\)](#)

刊名：[计算机技术与发展](#)

英文刊名：

年，卷(期)：2016 (2)

引用本文格式：[吴捷](#). [马小虎](#). [WU Jie](#). [MA Xiao-hu](#) [基于Hadamard变换和LU分解的盲水印算法](#)[期刊论文]-[计算机技术与发展](#) 2016 (2)