文章编号:1001 - 9081(2005)10 - 2365 - 02

一种基于混沌加密的 DCT 域数字图像水印算法

郑 融[1],金 聪[1,2],魏文芬[1],李 蓓[1]
(1. 华中师范大学 计算机科学系,湖北 武汉 430079;
2. 中国科学院 院信息安全国家重点实验室,北京 100039)
(rongzabc@ yahoo. com. cn)

摘 要:提出了一种基于混沌加密的 DCT 域数字图像水印算法。该算法利用 Logistic 映射生成一个随机序列,利用该随机序列对经过置乱处理的二值图像进行调制,最后将其嵌入到原始图像的低频系数中。仿真实验结果表明,实现的水印具有不可见性,而且对于常见的噪声、裁剪、JPEG 压缩具有较好的健壮性。

关键词:离散余弦变换;混沌序列;图像置乱;数字水印
中图分类号: TP391.41 **文献标识码**:A

Digital image watermark algorithm in DCT domain with chaotic encryption

ZHENG Rong[1], JIN Cong[1,2], WEI Wen-fen[1], LI Bei[1]
(1. *Department of Computer Science, Central China Normal University, Wuhan Hubei* 430079, *China;*
2. *State Key Laboratory of Information Security, Chinese Academy of Sciences, Beijing* 100039, *China*)

Abstract: A digital image watermark algorithm in DCT(Discrete Cosine Transform) domain with chaotic encryption was presented. A two-value image that had been dealt with by shuffle was modulated by a random watermark sequence created by using Logistic map, and then it was embedded to the low frequency coefficients of original image. Experimental results demonstrate that the watermark is invisible and robust against common noise, crop and JPEG compress etc.

Key words: DCT(Discrete Cosine Transform); chaotic sequence; image shuffle; digital watermark

0 引言

数字水印技术利用数字作品中普遍存在的冗余数据与随机性,向数字作品中加入不易察觉但可以判定区分的秘密信息水印(Watermark),从而起到保护数字作品版权或完整性的作用,其作为多媒体领域中知识产权保护的有效手段,正得到广泛的研究与应用。这种被嵌入的水印可以是一段文字、标识、ID 序列号等。

到目前为止,已经有许多文献对水印的嵌入和提取做过研究,数字水印的算法多种多样,大致可以分为空域法和频域法两种。频域法因其抗攻击、抗压缩、鲁棒性强,能将水印信号能量分布到所有像素上等特点,而被大多数算法广泛采用。常用的变换域有离散傅立叶变换(DFT)、离散余弦变换(DCT)以及离散小波变换(DWT)等。在这几种变换中二维 DCT 变换是目前最常用的有损数字图像压缩系统 JPEG 的核心,其技术成熟,在 DCT 域嵌入水印,对 JPEG 和 MPEG 压缩有较强的健壮性。因此,本文根据混沌序列对初始条件和系统参数敏感的特点,提出了一种在图像 DCT 变换的低频系数上嵌入水印的算法。

1 基于混沌序列调制二值数字图像水印

1.1 混沌序列

一个一维离散时间非线性动力系统定义为 $x_{k+1} = f(x_k)$;其中 $x_k \in V, k = 0,1,2,\cdots$ 称之为状态,$f: V \to V$ 是一个映射,反复应用 f,就可以得到一个序列 $\{x_k\}, k = 0,1,2,\cdots$,这个序列称为离散时间动力系统的一条轨迹。

Logistic 映射是一类简单却被广泛研究的混沌系统,它的定义为 $x_{k+1} = \mu x_k(1 - x_k), x_k \in (0,1), 0 \leqslant \mu \leqslant 4$。当 $3.569\,9456 < \mu \leqslant 4$ 时,Logistic 映射工作于混沌状态。由不同初始状态 x_0 生成的序列是非周期、不收敛、不相关的,并对初始值非常敏感。计算结果表明在进入混沌状态后,Logistic 映射产生的混沌序列具有 0 均值,δ - like 自相关及互相关为 0 的统计特性。该混沌序列具有以下优点:1)形式简单,只需要混沌映射参数和初始条件即可生成;2)对初始条件敏感,一般不同的初始值迭代得到的混沌序列都不相同,很难从一段有限长度推断混沌序列的初始条件;3)具有白噪声的统计特性,可以用于需要噪声调制的众多应用场合。

1.2 混沌水印调制信号

由以上分析可见,利用混沌序列作为水印调制信号具有简单易行、安全可靠的特点。利用给定密钥 key(实际为生成混沌序列的初始值)生成的混沌序列是一维的,如果要对二维的图像水印信号进行混沌调制,需要经过变换。生成混沌调制信号序列的方法[6]如下:

收稿日期:2005 - 03 - 31;**修订日期**:2005 - 06 - 02
基金项目:国家自然科学基金资助项目(10477007);湖北省教育厅重点基金资助项目(2003A012);中科院信息安全国家重点实验室开放基金资助项目(03 - 02)

作者简介:郑融(1980 -),女,湖北鄂州人,硕士研究生,主要研究方向:数字水印; 金聪(1960 -),女,上海人,教授,主要研究方向:信息隐藏、智能信息处理; 魏文芬(1979 -),女,湖北公安人,硕士研究生,主要研究方向:计算机视觉; 李蓓(1981 -),女,河南信阳人,硕士研究生,主要研究方向:信息安全.

1）利用 Logistic 映射生成实数值序列 $\{x_k; k-1,2,\cdots\}$，从序列 x_k 中选取 $M_1 \times M_2$（水印大小）个元素，本文使用 Logistic 映射的初始条件为 $x_0 = 0.123$，系统参数为 4；

2）通过定义阈值函数 T 经过阈值变换后得到二值混沌序列 $\{T(x_k); k = 1,2,\cdots,M_1 \times M_2\}$，其中 T 可以定义为当 $x < \tau$ 时 $T(x_k) = 0$；而当 $x \geqslant \tau$ 时 $T(x_k) = 1$。

3）将 $T(x_k)$ 转换得到二维混沌调制信号 $h(i,j)$。

1.3 混沌序列调制二值数字图像水印

为了提高水印的加密性和提取出的水印的视觉效果，首先将二维二值水印信号 W_0（本文使用的水印图像为 $M_1 \times M_2$ 的二值图像）通过 Arnold 变换（变换次数可作为密钥的一部分）得到 W，然后对变换水印 W 进行混沌序列调制 $w(i,j) \oplus h(i,j)$，最终得到基于混沌序列调制加密的二值图像水印。

2 DCT 域图像水印嵌入算法

2.1 DCT 域水印嵌入

DCT 变换域算法的基本思想是利用扩频（Speread Spectrum）通信的原理来提高数字水印的稳健性。Cox 等人提出了比较具有代表性的一种观点，为使水印稳健，水印信号应该嵌入到原始图像中对人的视觉感觉最重要的部分，在频率空间中，这种最重要的部分就是低频分量。将水印嵌入到 DCT 变换的低频系数中，图像的低频能量集中了原图的绝大部分能量，攻击者在破坏水印的过程中，不可避免会引起图像质量下降，水印嵌入于此具有足够的稳健性，而且图像的低频系数具有较大的值，水印信号嵌入后对图像影响较小，有利保证水印的不可见性。在具体实现时，需要对原始图像和水印图像进行分块。原始图像（$N_1 \times N_2$）子块的大小为 8×8，相应的水印图像子块的大小为 $(8 \times \frac{M_1}{N_1}) \times (8 \times \frac{M_2}{N_2})$，这样保证了原始图像和水印图像具有相同数目的子块。对原始图像进行分块 DCT 变换，对每一 8×8 分块 DCT 系数按照降序排好序，选出从某个低频系数（即 1 ~ 21 个低频系数中的某个）开始的 $64 \times \frac{M_1 \times M_2}{N_1 \times N_2}$ 个系数，然后将对应块的水印信号嵌入到其中。

2.2 水印嵌入

水印嵌入的具体过程如下：

1）对原始图像分块，子块大小为 8×8，每个分块互不重叠；

2）对经过混沌加密的水印图像进行分块，使其与原始图像具有相同数目的子块；

3）对原始图像的每个子块进行二维 DCT 变换；

4）对每一个 DCT 变换后的子块，根据以下公式嵌入一位水印：

$$N'_k(i,j) = N_k(i,j)(1 + \alpha \times W_k(i,j))$$

其中 $N_k(i,j)$ 是原始图像的 DCT 系数，$N'_k(i,j)$ 是嵌入水印后图像的 DCT 系数，$W_k(i,j)$ 是与原始图像块号相同的水印信息，α 是水印嵌入强度，α 的取值依具体图像而定，本文 $\alpha = 0.1$，k 为 DCT 低频部分从 6 ~ 9；

5）对嵌入水印后的 DCT 系数进行 IDCT 变换，重建图像，得到嵌入水印后的图像。

2.3 水印的提取

一般水印的提取与水印的嵌入是互逆过程。

水印提取步骤如下：

1）将待检测的图像同嵌入水印时一样进行分块，子块大小为 8×8，并对子块进行 DCT 变换；

2）将原始图像进行同样分块以及 DCT 变换；

3）原始图像和待检测图像进行运算，求出各部分子块嵌入水印的估计值，运算公式：

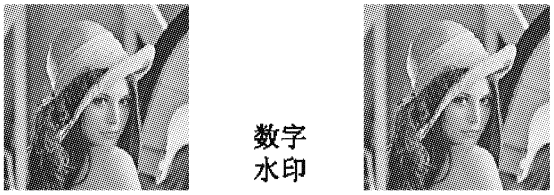
$$W_k(i,j) = (N'_k(i,j) - N_k(i,j))/(\alpha \times N_k(i,j))$$

4）将各水印块合并，得出嵌入的经过混沌加密的水印图像；

5）对该图像进行混沌加密水印的逆过程，得到原始的二值水印图像。

3 实验结果与讨论

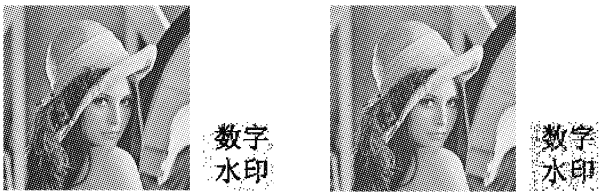
本文选择 256 级灰度图像 Lena 作为原始图像，大小为 256×256；水印图像是二值图像，大小为 64×64。实验结果如图所示。



(a) 原始图像 (b) 二值图像 (c)嵌入水印后的图像

图 1 进行测试前的结果

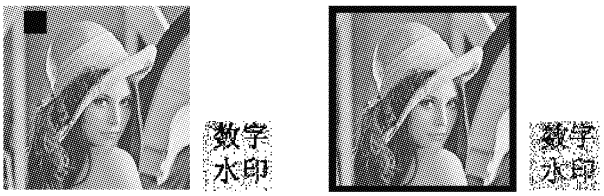
1）噪声攻击：向图像中分别添加噪声强度为 0.02 的随机噪声和噪声强度为 0.002 的椒盐噪声后，仍能提取出水印，抗噪声攻击性能较好。



(a) 添加随机噪声后的图像及提取的水印 (b) 添加椒盐噪声后的图像及提取的水印

图 2 噪声攻击实验结果

2）抗裁剪攻击：在图像上分别裁剪（10:40,30:60）和[(1:256,1:10),(1:10,1:256),(1:256,246:256),(246:256,1:256)]区域后，仍能正确提取出水印。

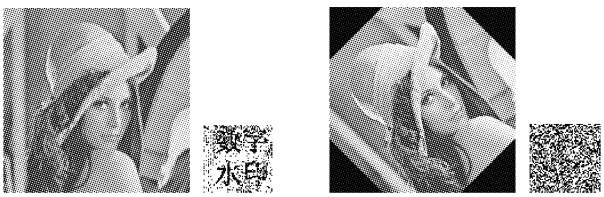


(a) 裁剪后的图像及提取水印 (b) 裁剪后的图像及提取水印

图 3 抗裁剪攻击实验结果

3）抗 JPEG 压缩：对图像进行压缩比为 3/4 的 JPEG 压缩后，能正确提取出水印。

4）抗旋转攻击：该系统抗旋转攻击的性能很差。



(a) 8JPEG压缩后的图像及提取的水印 (b) 旋转45度后的图像及提取的水印

图 4 抗旋转攻击实验结果

（下转第 2373 页）

法[3,9](嵌入服从标准正态分布的 1 000 个信号序列,alpha = 0.1);盲扩谱方法[4](嵌入服从标准正态分布的 16000 个信号序列);基于 8×8 DCT 块的扩谱方法[5](容量 0.05bpp,每 DCT 块嵌入 3 bits);基于 8×8 DCT 块量化索引调制(QIM)方法(容量 0.1bpp,每 DCT 块嵌入 6 bits);最低位平面(LSB)方法(容量 0.3bpp)。

表 6 是空域矩和频域矩对于 CorelDraw 图像库的隐写分析结果。表 7 是 Farid 方法和 Harmsen 方法对于 CorelDraw 图像库的隐写分析结果。

表 6　空域矩特征和频域矩特征隐写分析对 CorelDraw 的测试结果

数据隐藏方法	空域矩 39 维			频域矩 39 维(本文方法)		
	原图识别率%	嵌入图识别率%	总识别率 %	原图识别率%	嵌入图识别率%	总识别率 %
Cox	62.5	51.6	57.1	94.1	96.0	95.0
Piva	77.2	69.8	73.5	88.5	96.6	92.6
Huang	93.0	90.8	92.0	93.3	98.4	95.9
QIM	90.0	86.0	88.0	97.2	99.0	98.1
LSB	87.6	32.6	60.1	93.1	93.6	93.3
综合	54.7	74.8	71.5	87.4	88.8	88.5

表 7　Farid[1] 和 Harmsen[2] 隐写分析对 CorelDraw1 096 的测试结果

数据隐藏方法	Farid 方法 72 维			Harmsen 方法 3 维		
	原图识别率%	嵌入图识别率%	总识别率%	原图识别率%	嵌入图识别率%	总识别率%
Cox	75.3	52.9	64.1	51.6	85.1	68.4
Piva	86.4	89.2	87.8	91.4	52.4	71.9
Huang	92.0	61.3	76.6	96.0	64.0	80.0
QIM	99.3	100	99.6	91.8	50.6	71.2
LSB	89.8	52.7	71.3	80.9	41.1	61.0
综合	86.3	53.0	80.7	97.8	80.1	83.3

4　结语

1) 本文第一次提出使用图像小波子带系数直方图频域多阶统计绝对矩作为特征,进行图像隐写分析,取得良好的分类性能;

2) 从理论和实际两方面论证了,对于图像隐写分析,直方图频域矩优于直方图空域矩;

3) CorelDraw 1 096 图像库测试结果表明,本文方法优于目前其他的通用隐写方法。

参考文献:

[1] FARID H. Detecting hidden messages using higher-order statistical models[A]. In: Proc. of the IEEE Int'l. Conf. on Image Processing 02[C], Vol II. New York: IEEE, 2002. 905 - 908.

[2] HARMSEN JJ. Steganalysis of Additive Noise Modelable Information Hiding [D]. Rensselaer Polytechnic Institute, Troy, New York , May 2003.

[3] COX IJ, KILIAN J, LEIGHTON T, *et al.* Secure Spread Spectrum Watermarking for Multimedia[J]. IEEE Trans. on Image Processing, 1997, 6(12): 673 - 1687.

[4] PIVA A, BARNI M, BARTOLINI E, *et al.* DCT-based Watermark Recovering without Resorting to the Uncorrupted Original Image [A]. Proceedings of the 1997 International Conference on Image Processing (ICIP'97) [C], 3 - Vol. 1 , P. 520.

[5] HUANG J, SHI YQ. An adaptive image watermarking scheme based on visual masking[A]. IEE Electronic Letters[C], 1998, 34(8): 748 - 750.

[6] DUDA RO, HART PE, STORK DG. Pattern Classification, Second Edition[M]. John Wiley & Sons, 2001.

[7] CorelDraw Software[EB/OL]. http://www.corel.com, 2005.

[8] 苏淳. 概率论[M]. 北京:科学出版社, 2004.

[9] 刘绍辉, 姚鸿勋, 高文, 等. 针对小波域量化隐藏方法的图像监测技术研究[J]. 通信学报, 2004, 25(7): 71 - 77.

[10] SHI YQ, GUO RX, CHENG YY, *et al.* Effective Steganalysis Based on Statistical Moments of Wavelet Characteristic Function [A]. International Conference on Information Technology Coding and Computing (IEEE ITCC 2005) [C], Las Vegas, NV, USA, 2005.4 - 6.

[11] SHI YQ, GUO RX, ZOU D, *et al.* Steganalysis Based on Moments of Characteristic Functions Using Wavelet Decomposition, Prediction-Error Image, and Neural Network[A], International Conference on Multimedia & Expo (IEEE ICME 2005) [C], Amsterdam, The Netherlands, 2005.6 - 8.

[12] GUO RX, SHI YQ, GAO J, *et al.* Steganalysis Based on Multiple Features Formed by Statistical Moments of Wavelet Characteristic Functions[A]. The 7th Information Hiding Workshop (IH05) [C]. Barcelona, Catalonia, Spain, 2005.6 - 8.

(上接第 2366 页)

综合上述的分析可知:本水印系统对噪声、裁剪、JPEG 压缩有较强的稳健性,在旋转处理后几乎不能检测出水印信息。

4　结语

本文基于混沌序列和置乱提出了一类二值图像水印改进算法,算法具有以下特点:1) 应用混沌序列加密和空域变换方法,安全性高;2) 水印嵌入到原始图像的低频区域,稳健性较好;3) 水印的嵌入和提取计算复杂度小,算法简单可靠。

参考文献:

[1] 王颖, 黄志蓓. 数字水印[M]. 北京: 电子工业出版社, 2003.

[2] 冯登国. 密码学原理与实践[M]. 第 2 版. 北京: 电子工业出版社, 2003.

[3] NIKOLAIDIS N, TSEKERIDOU S, NIKOLAIDIS A, *et al.* Applications of chaotic signal processing techniques to multimedia Watermark[J]. Proceedings of the IEEE workshop on Nonlinear Dynamics in Electronic Systems, Catania Italy, May 18 - 20, 2000, 1 - 7.

[4] SCHMITZ R. Use of chaotic dynamical systems in cryptography[J]. J. Franklin. Institute, 2001.338 (4): 429 - 441.

[5] OGORXALEK KMP. Special Issual on Chaos Synchronization and Control: Theory and Application[J]. IEEE Transactions on Circuits and Systems, 1997, 44(10): 853 - 1039.

[6] 张志明, 王磊. 基于混沌加密的 DCT 域图像水印算法[J]. 计算机工程, 2003, 29(17): 10.

[7] 孙兆林. MATLAB 6.x 图像处理[M]. 北京: 清华大学出版社, 2004.

[8] 曹芝兰. 数字图像加密与水印技术的研究[D]. 武汉: 湖北大学硕士学位论文, 2004.