第 27 卷第 5 期　　四川理工学院学报(自然科学版)　　Vol. 27　No. 5
2014 年 10 月　　Journal of Sichuan University of Science & Engineering(Natural Science Edition)　　Oct. 2014
文章编号:1673-1549(2014)05-0058-06　　DOI:10.11863/j.suse.2014.05.14

基于 DCT 和 CNN 混沌系统的彩色数字水印加密新算法

赵国敏[a], 李国东[a], 朱文辉[b]

(新疆财经大学 a. 应用数学学院;b. 经济学院, 乌鲁木齐 830012)

摘　要:数字水印技术作为抵抗多媒体盗版的最后一道技术防线,具有广泛的应用前景和巨大的经济价值。基于离散余弦变换(DCT)以及细胞神经网络(CNN)混沌理论提出了一种数字水印加密新算法。算法分两步进行,首先是利用 5 阶细胞神经网络混沌系统产生的随机序列辅助某种运算对彩色水印图像加密,然后利用分块离散余弦变换将加密以后的彩色水印图像嵌入到载体彩色图像中,以此来实现水印加密以及嵌入的过程。在仿真实验基础上,通过指标 PSNR 和 NC 的定量分析,结果证明新算法具有较强鲁棒性,不可感知性和安全性。

关键词:数字水印;离散余弦变换(DCT);细胞神经网络(CNN);超混沌

中图分类号:TP309.7　　**文献标志码**:A

引　言

数字水印已成为人们解决数字产品版权问题的一个重要解决方法,并且该方法在图像保护研究领域已得到广泛研究而被提上日程。数字水印原理是向作为载体的视频、音频及图像文件中添加一些数字信息而不影响载体信息质量,同时添加的这些数字信息还可以在载体文件中重新无失真获得,其实质是一种信息隐藏技术。通过水印的嵌入与提取来达到数字产品版权保护及使用的目的。为了进一步提高网络版权的安全性,防止第三方对版权产品的窃取和破坏,还可以对数字版权产品实施加密预处理技术。

目前,数字水印算法总体可分为空间域和变换域两大类。空间域算法直接作用于载体图像以达到隐藏水印信息的目的,该算法简单易行,但攻击鲁棒性能差。而变换域算法是在载体图像的某种变换域上实现水印嵌入,其变换方法有离散傅立叶变换(Discrete Fourier Transform,DFT)、离散余弦变换(Discrete Cosine Transform,DCT)、离散小波变换(Discrete Wavelet Transform,DWT)等。变换域算法符合数字水印鲁棒性、安全性、透明性及保真性等性能要求,是目前主要的研究方向。由于 DCT 变换后矩阵特征向量和图像及语音信息的矩阵相似程度很大,因此 DCT 变换被认为是对图像以及音频信息的最佳变换方法。

在变换域水印方法中,目前已出现了众多对 DCT 变换的数字水印算法,随着数字水印应用范围越来越高,水印技术也逐步趋于成熟。随着电子技术的发展,彩色图像数字水印问题越来越受到重视,是目前研究的重点领域[1-2]。李诺等人针对 YIQ 色彩空间,将灰度图像水印信号自适应嵌入载体的亮度分量 Y 的 DCT 系数中的水印方法[3];相继白香芳等人针对于 HSI 色彩空间提出把原始图像各分量通过分块 DCT 嵌进水印的数字水印算法[4]。文献[3-4]是基于 DCT 变换把 Amold 置乱后的二值图像通过某种运算成功嵌入彩色载体图像中,通过

收稿日期:2014-04-16

基金项目:国家教育部人文社会科学基金(13YJAZH040);新疆维吾尔自治区高校科研计划项目(XJEDU2013I26)

作者简介:赵国敏(1988-),女,河北邢台人,硕士生,主要从事数据挖掘与分析方面的研究,(E-mail)zhaoguominzhaomin@126.com

李国东(1972-),男,黑龙江哈尔滨人,教授,博士,主要从事图像处理、数据挖掘与分析方面的研究,(E-mail)lgdzhy@126.com

实验证明水印算法某种程度上具有较好鲁棒性和安全性。尽管 Amold 置乱 N 次后可以得出原始图像,但算法针对的是二值水印图像,对于彩色水印算法不再适用。本文在此基础上,针对 RGB 色彩空间提出一种基于分块 DCT 变换方法,将加密预处理后的 RGB 彩色水印信息嵌入到 RGB 彩色载体图像中的水印算法。

1　基于 DCT 数字水印嵌入原理

离散余弦变换是数字图像预处理过程中经常用到的一种正交变换方法,且为可逆变换,变换函数是余弦函数。大小为 $M \times N$ 的数字图像 $I(m,n)$ 是一个二维矩阵,其二维 DCT 变化可描述为:

$$F(s,t) = c(s)c(t)\frac{2}{\sqrt{MN}}\sum_{m=0}^{M-1}\sum_{n=0}^{N-1}f(m,n) \times \cos\left[\frac{\pi}{2M}(2m+1)s\right]\cos\left[\frac{\pi}{2N}(2n+1)t\right] \quad (1)$$

DCT 反变换即 IDCT 表述为[5]:

$$F(m,n) = \frac{2}{\sqrt{MN}}\sum_{m=0}^{M-1}\sum_{n=0}^{N-1}c(s)c(t)F(s,t) \times \cos\left[\frac{\pi}{2M}(2m+1)s\right]\cos\left[\frac{\pi}{2N}(2n+1)t\right] \quad (2)$$

式中:

$$c(s) = \begin{cases} 1, & s = 1,2,\cdots,M-1 \\ \frac{1}{\sqrt{2}}, & s = 0 \end{cases}$$

$$c(t) = \begin{cases} 1, & t = 1,2,\cdots,N-1 \\ \frac{1}{\sqrt{2}}, & t = 0 \end{cases}$$

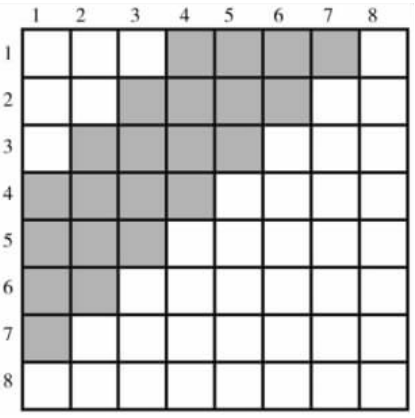
当式(1)中 s、t 不断增大时,相应的余弦函数的频率也不断增大,得到的系数可认为就是原始图像信号在频率不断增大的余弦函数上的投影,所以也被称为低频系数、中频系数和高频系数。

对一副图像进行离散余弦变换以后,图像的重要信息都集中在 DCT 变换系数中的一小部分区域中,因此 DCT 变换是有损图像压缩的核心组成部分,而这“一小部分”就是指的低频部分。由于中、低频系数所含有的原始信号成份较多,所以由其反变换重构图像就能得到图像的近似部分。高频系数是在众多正交的余弦函数上投影的加权,是这些不同频率的余弦信号一起来刻画原始信号的结果,图像近似的部分在这些函数上被相互抵消了,剩下的就是图像的细节部分了。

本文通过对 lena 灰度原始图像(图 1(a))做 DCT 变换得到 DCT 频谱图(图 1(b))。观察 DCT 变换系数发现,从左上到右下方向 DCT 系数绝对值是递减的,因此可以得出 DCT 低频系数分布在变换矩阵的左上部,高频系数分布在变换矩阵的右下部,低频系数的绝对值大于高频系数的绝对值。

(a)lena原图

(b)lena图像DCT频谱图



(c)块DCT系数的中频位置

图 1　lena 图像 DCT 变换实验

由于 DCT 变换系数的低频系数几乎包含了图像的全部信息,其统计特性逼近原始图像,这一部分是人类视觉最为敏感的地带,为了不影响原始图像的质量,此频率带不宜添加水印。高频成分包含图像的细节部分,主要是图像的边缘及纹理信息,把水印嵌入至高频系数

区域时会因为低通滤波和量化等操作中损失掉一些信息,因此加入到高频系数中水印的鲁棒性较差。本文使用折中方法,选择中频系数中的固定位置来嵌入水印[6],将水印嵌入到 DCT 子块的中频系数,如图 1(c)阴影部分所示。

2 细胞神经网络超混沌系统

混沌是自然界中普遍存在的一种无规则、类随机的现象,也就是说人们不能捕获其下一时刻的运动轨迹,这种类随机的混沌现象比较适合于保密通信领域的应用中。蔡少堂在 1988 年首次提出细胞神经网络(Cellular Neural Network ,简称 CNN) 理论,它是一种局部互连的神经网络系统[7]。该系统具有极其复杂的动力学行为,能够实时、高速、并行处理信号,且易于超大规模电路的实现。研究证明这种复杂系统在变量维数变化过程中很大参数范围内可以产生混沌现象,因此利用该系统所产生的类随机的混沌序列对图像加密很大程度增强图像的安全性。

细胞神经网络状态方程:[8-9]

$$\frac{\mathrm{d}x_j}{\mathrm{d}t} = -x_j + a_j f(x_j) + G_o + G_s + \tilde{I}_j \tag{3}$$

$$f(x_j) = \frac{1}{2}(|x_j + 1| - |x_j - 1|) = \begin{cases} 1 & x_j \geqslant 1 \\ x_j & |x_j| < 1 \\ -1 & x_j \leqslant -1 \end{cases} \tag{4}$$

其中, x_j 表示第 j 个细胞的状态; a_j 为常数; $\tilde{I}_j$ 为阈值常数; $f(x_j)$ 为细胞输出,是状态变量 x_j 的分段线性函数,见式(4); G_o 和 G_s 分别是所连接细胞的输出和状态变量 x_j 的线性组合。

由式(3)与式(4)可知五阶的全互连 CNN 动态模型的方程式为:

$$\frac{\mathrm{d}x_j}{\mathrm{d}t} = -x_j + a_j f(x_j) + \sum_{k=1}^{5} A_{jk} f(x_k) + \sum_{k=1}^{5} S_{jk} x_k + \tilde{I}_j (j = 1,2,\cdots,5) \tag{5}$$

其微分方程组各系数取值分别为:

$$S_k = \begin{bmatrix} 1 & 0 & -1 & -1 & 0 \\ 0 & 3 & 1 & 0 & 0 \\ 12 & -13 & 1 & 0 & 0 \\ 90 & 0 & 0 & -92 & -2 \\ 0 & 0 & 14 & 0 & -1 \end{bmatrix}$$

$$a_j = \begin{cases} a_1 = 0 \\ a_2 = 0 \\ a_3 = 0 \\ a_4 = 2 \\ a_5 = 0 \end{cases}$$

$$\tilde{I}_j = \begin{cases} \tilde{I}_1 = 0 \\ \tilde{I}_2 = 0 \\ \tilde{I}_3 = 5 \\ \tilde{I}_4 = 0 \\ \tilde{I}_5 = 1 \end{cases}$$

$$A_{jk} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 200 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

由此可得 CNN 微分方程组:

$$\begin{cases} \frac{\mathrm{d}x_1}{\mathrm{d}t} = -x_3 - x_4 \\ \frac{\mathrm{d}x_2}{\mathrm{d}t} = 2x_2 + x_3 \\ \frac{\mathrm{d}x_3}{\mathrm{d}t} = 12x_1 - 13x_2 + 5 \\ \frac{\mathrm{d}x_4}{\mathrm{d}t} = 90x_1 - 93x_4 - 2x_5 + 202f(x_4) \\ \frac{\mathrm{d}x_5}{\mathrm{d}t} = 14x_3 - 2x_5 + 1 \end{cases} \tag{6}$$

利用四阶龙格库塔算法求解方程(6),可得产生的混沌吸引子,从而可知系统正处于一种类随机运动中。格里波基在 1983 年已经证明只要李雅普诺夫指数中有大于零的数就可以确定混沌现象的存在。当大于零的李雅普诺夫指数个数大于等于 2 时就可以证明系统处于超混沌状态。当选择 [0.2,0.2,0.2,0.2,0.2] 作为式(6)的初始条件,可得到两个大于零的指数,分别为 4.9583 和 2.4877,因此可以证明此时系统运动轨迹为超混沌现象,所产生的序列更为随机。利用 CNN 系统产生更为随机的超混沌序列,在某种程度上增强了水印加密的安全性。

3 基于 DCT 数字水印实现

本文选择 256 × 256 × 3 大小的载体彩色图像以及 32 × 32 × 3 的水印彩色图像作为训练样本。假设上述水印嵌入位置、5 阶细胞神经网络系统和初始条件作为密钥信息,而发送者和接受者双方共同享有密钥信息,也

就是说发送方利用密钥信息加密,接收方利用相同的密钥信息解密。本文中提出基于 DCT 和 CNN 数字水印加密算法实现步骤如下:

Step1:读取 RGB 水印图像 water 并将 R,G,B 三色分离。

Step2:利用 CNN 系统(6)生成混沌序列,任选其中三个向量作为加密序列,不失一般性,本文选择加密序列 $x1,x2,x3$, 首先将其重排成 32×32 的矩阵,按以下方法加密水印彩色图像的 R、G、B 层,其中选取 $k=10$,

$$waterr = \mathrm{mod}(waterr + round(k * x1),256)$$

$$wateg = \mathrm{mod}(wateg + round(k * x1),256)$$

$$waterb = \mathrm{mod}(waterb + round(k * x1),256)$$

Step 3:读取 RGB 载体图像,将 R、G、B 三色分离,并将分离后的每层完全分割为互不覆盖的(8×8)图像块,然后对每块做 DCT 变换,利用生成的变换系数以及 step2 中生成的加密水印层按嵌入算法嵌入水印,其中 α 为嵌入强度,水印嵌入位置为每块的第 2 行第 6 列,接着对嵌入水印的图像块做 IDCT 变换,最后合并图像块。

```
for p = 1:32
for q = 1:32
x = (p - 1) * 8 + 1; y = (q - 1) * 8 + 1;
block_inputr = inputr(x:x + 8 - 1, y:y + 8 - 1);
block_inputr = dct2(block_inputr);
for i = 1:8
for j = 1:8
if i = =2 && j = =6 block_inputr1(2,6) = block_inputr(2,6) + α * w aterr(p,q);
else block_inputr1(i, j) = block_inputr(i, j);
end
end
end
block_inputr2 = idct2(block_inputr1);
inputr1(x:x + 8 - 1, y:y + 8 - 1) = block_inputr2;
end
end
```

Step 4:水印嵌入。将以上生成的嵌入水印的图像层(R、G、B)合并成嵌入水印的彩色图像,如图 2 所示。

Step 5:提取水印。水印的提取过程为水印嵌入过程的逆过程,如图 3 所示。

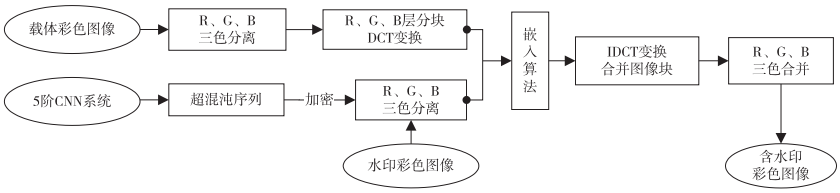


图 2　水印嵌入过程流程图

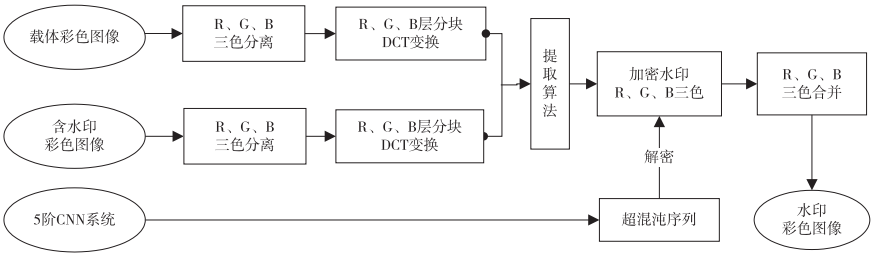


图 3　水印提取过程流程图

4　实验仿真及结果分析

为了提高可信度,本文定量分析水印嵌入以及提取的效果。通常把峰值信噪比(*PSNR*)以及相关系数(*NC*)作为数字图像被嵌入以及被提取的衡量指标[10]。

(1) 峰值信噪比

峰值信噪比(*PSNR*)是衡量水印算法不可感知性的评价指标,值越高,不可见性越好,其定义为:

$$PSNR = 10\log_{10}\frac{M * N * 255^2}{\sum_{x=1}^{M}\sum_{y=1}^{N}[f(m,n) - f_W(m,n)]^2} \quad (7)$$

其中,M 和 N 分别为图像的长和宽,$f(x,y)$ 为原始图像矩阵,$f_W(x,y)$ 为嵌入水印的图像矩阵。*PSNR* 值主要受嵌入强度的影响,表 1 分别给出了训练样本测试过程中不同嵌入强度 α 的 *PSNR* 值。可见随着嵌入强度 α 的增加,*PSNR* 值在减小。同时还发现 α 越小检测水印难度越大,α 越大嵌入水印后图像的视觉效果越差。一般,

要达到图像质量主观上不容易被人察觉的效果,其 *PSNR* 值要大于 20,但实际应用中,我们有更高要求,即要求 *PSNR* 值大于 37[10]。文献[11]在嵌入强度 α = 0.15 时对不同图像进行实验,计算得到其 *PSNR* 值在 39 附近均达到较好效果,鉴于此本文选择嵌入强度 α 为 0.2。

表 1 嵌入强度 α 与 *PSNR* 关系

α	*PSNR*	α	*PSNR*
0.05	50.9643	0.25	37.7167
0.1	45.3565	0.3	36.2283
0.15	41.8957	0.35	34.9498
0.2	39.5283	——	——

基于以上要素,本文进行实验仿真。选取彩色图像如图 4(a)以及水印彩色图像如图 4(b)作为训练样本,按照本文算法实现步骤嵌入水印。实验结果见图 4,其中图 4(c)为加密后的水印图像,图 4(d)为加水印后的彩色图像,图 4(e)为提取出来的水印图像。可见经过加密后的水印已看不出原始的水印图像,提取出的水印和原图基本一致。

(a)原始图像 (b)水印图像 (c)加密水印图像

(d)加水印后图像 (e)提取水印图像

图 4 实验结果

(2) 相关系数

相关系数(*NC*)是衡量数字水印鲁棒性的指标,用来检测嵌入水印图像以及提取水印图像之间的相似程度。*NC* 值越大,表明提取出的水印与原来的水印相似程度越高,效果越好,反之,值越小,表示相似程度越低。

$$NC = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n} W(i,j)W'(i,j)}{\sum_{i=1}^{m}\sum_{j=1}^{n} W(i,j)^2} \tag{8}$$

其中,m 和 n 分别为水印图像的长和宽,$W(i,j)$ 为水印图像矩阵,$W'(i,j)$ 为提取水印的图像矩阵。

本文选择对含水印的彩色图像进行各种攻击的方法来检验算法鲁棒性。图 5 分别给出了含水印图像在受到不同类型攻击后提取的水印图像效果图,从图可以看出水印在受到攻击后提取的水印不同程度受损,但很容易辨别出水印图像。用相关系数指标来衡量提取的水印和原始水印之间差距结果见表 2。

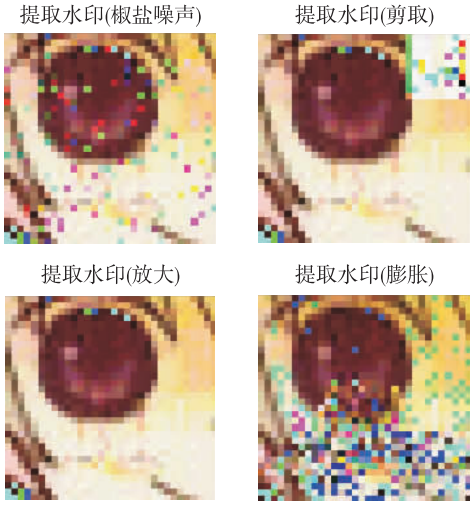


图 5 受到各种攻击后提取的水印

表 2 受到攻击后提取水印与原始水印的相关系数

攻击类型	噪声(椒盐)攻击	剪切(右上)攻击	伸缩(放大)攻击	膨胀攻击
NC	0.7856	0.7683	0.8131	0.6905

从表 2 结果可以看出,提取出来的水印图像和原始水印图像之间相关系数都在 70% 左右,有的甚至达到了 80%。一般认为相似程度达到 60% 就可以证明提取效果较好。因此可以证明本文所设计的算法对常见的几种攻击方式都具有较好的鲁棒性,安全程度更高。

5 结 论

(1)本文基于离散余弦变换和细胞神经网络混沌提出了一种加密彩色图像到彩色载体图像中的数字水印加密新算法,实验结果证明该算法具有较好的不可感知性和鲁棒性。

(2)本文算法中密钥空间巨大,增强了水印算法的安全性。其中密钥包括细胞神经网络系统中的 60 个参数和系统的初始条件 5 个,以及在加密过程中用到的常数 k,另外考虑到密钥敏感度[12],仅细胞神经网络系统产生的密钥空间就达到 6.5×10^{17},能有效抵抗穷举攻击,增强图像安全程度。

(3)在水印嵌入时,本文选择了一个全局嵌入强度 α,并没有考虑不同 DCT 变换系数应该选择不同的嵌入

强度 α, 这是需要继续研究的问题。

参 考 文 献:

[1] 赵玉霞,屈正更.基于混沌序列与 LWT 的彩色图像数字水印新算法[J].西北大学学报:自然科学版,2013,43(3):371-375.

[2] 朱 光,师 文,朱学芳,等.结合 SURF 特征的多功能彩色图像水印算法[J].中国图像图形学报,2013,18(12):1694-1702.

[3] 李 诺,闫德勤.一种二维 DCT 彩色图像数字水印的新算法[J].计算机工程与应用,2007,43(2):43-45.

[4] 白香芳,李晓静.基于 DCT 技术彩色图像水印算法的研究[J].辽宁师范大学学报:自然科学版,2013,36(2):178-182.

[5] 王建哲,姜昱明.一种基于 DCT 变换的数字水印技术[J].计算机工程与应用,2002(6):104-105.

[6] 杨 焰,刘 炜.基于 DCT 的数字水印加密与解密技术[J].中南林业科技大学学报,2011,31(11):203-207.

[7] Chua L O,Yang L.Cellular neural network: theory[J]. IEEE Transactions on Circuit and System,1988,35(10):1257-1272.

[8] 朱艳平,张小红.基于细胞神经网络的图像加密新算法[J].江西理工大学学报,2008,29(1):27-30.

[9] 刘玉明,周冬明,赵东风.基于细胞神经网络超混沌特性的图像加密[J].云南大学学报:自然科学版,2007,29(4):355-358.

[10] 庄晓梅.基于 DCT 域数字图像鲁棒水印方案的研究及实现[D].济南:山东师范大学,2013.

[11] 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.

[12] 赵国敏,李国东.基于细胞神经网络混沌特性的图像加密技术应用研究[J].绵阳师范学院学报,2014,33(2):92-97.

New Algorithm of Color Digital Watermark Encryption Based on DCT and CNN Chaotic System

ZHAO Guomin[a], *LI Guodong*[a], *ZHU Wenhui*[b]

(a. School of Application Mathematic; b. School of Economics, Xinjiang University of Finance & Economics, Urumchi 830012, China)

Abstract: As the last line of defense technology against the multimedia piracy, digital watermarking technology has wide application prospect and great economic value. A new digital watermarking encryption algorithm is proposed based on the discrete cosine transform (DCT) and cellular neural network (CNN) chaotic theory. The algorithm is consisted of two steps to complete the process of watermark encryption and embedding. Firstly, the random sequences are generated by the 5 order cellular neural network chaotic system and are operated to achieve the encryption of color watermark image. Then the encrypted color watermark image is embedded into the host image by the block method of discrete cosine transform. At last, the simulation experiments are done, and the results show that the watermarking algorithm has strong robustness, imperceptibility and security through the quantitative analysis of the indexes of PSNR and NC.

Key words: digital watermarking; discrete cosine transform (DCT); cellular neural network (CNN); hyper chaos