doi: 10.3969/j.issn.1006-1576.2011.05.013

一种新型的图像哈希算法

陈青华
（山东省工会干部管理学院 信息工程学院，济南 250100）

摘要：为了提高图像哈希方法的鲁棒性，提出一种基于 BP 神经网络的新型图像哈希算法，首先利用图像像素矩阵和构造的函数来训练 BP 神经网络，再将图像进行离散小波变换，利用低频分量来组成矩阵，最后利用已经训练好的 BP 神经网络来产生哈希序列。仿真结果表明，该算法对 JPEG 压缩、图像滤波等内容保持操作具有较好的稳健性，具有较好的应用价值。

关键词：图像哈希算法；图像认证；BP 神经网络
中图分类号：TP183　　**文献标志码**：A

A New Style Image Hash Algorithm

Chen Qinghua
(College of Information Engineering, Shandong Union Cadre Management College, Jinan 250100, China)

Abstract: To improve the robust of the image hash method, a new style image hash algorithm based on BP neural network was proposed. Firstly, the image pixel matrix and a constructed function was used to train the back propagation BP neural network, and then the low-frequency components obtained by the discrete wavelet transform was used to composes the matrix, the image hash sequence was generated by the well-trained back propagation BP neural network in the end. The experimental results indicate that the proposed hash method is robust against content-preserving modifications (such as JPEG compression, image filtering) and has good application value.

Keywords: image Hash algorithm; image authentication; BP neural network

0　引言

互联网上的海量数字图像给人们的生活工作提供了便利。与此同时，图像的海量存储、快速检索和图像版权保护等问题也日趋重要。哈希技术可以将任意分辨率的图像数据转化为几百或几千比特的二值序列，可极大地减少图像搜索的时间，降低存储图像的介质成本，同时，其鲁棒性的特点也保证它可以抵抗多种不同类型的攻击，可以有效地解决在线图像检索和认证等领域的问题。

传统的图像哈希方法是基于密码学的，具有对原始数据比特过于敏感的缺陷。近几年，鲁棒性图像哈希方法引起了国内外学者的广泛关注，文献[1]提出了一种基于非负矩阵分解和主成分分析的感知哈希方法，通过对哈希生成两阶段框架的详细分析，非负矩阵分解被设计用来捕获图像的局部信息，而主成分分析用来捕获全局信息和信息压缩，图像之间的相似程度通过哈希的归一化相关值来确定；文献[2]通过利用图像离散小波变化低频系数的感知不变性生成安全的哈希序列索引，然后用标准化后的离散小波变化低频系数矩阵和基于密钥种子的随机数矩阵为数字图像生成哈希序列，从而构造了一种鲁棒的图像感知哈希算法；文献[3]提出了一种新的基于完备正交函数系统的图像哈希方法，该方法首先将原始图像强化，然后提取完备正交函数变换域上的系数生成哈希值；文献[4]提出了一种组合非负矩阵分解和奇异值分解的感知哈希方法，图像首先被分割成依赖于密钥的重叠图像块，每块进行非负矩阵分解得到表征图像局部特征的系数矩阵，然后对其进行奇异值分解取最大的奇异值矢量构成哈希序列。上述方法可以在一定程度上提高哈希算法的鲁棒性，但都不同程度上存在哈希处理时间过长、不能自适应处理图像内容的变化等缺陷。

前馈型神经网络（back propagation neural networks）是一种按误差反向传播算法训练的多层前馈网络，能学习和存贮大量的输入—输出模式映射关系，无需事前揭示描述这种映射关系的数学方程。它的学习规则是使用最速下降法，通过反向传播来不断调整网络的权值和阈值，使网络的误差平方和最小。鉴于此，笔者提出了一种基于 BP 神经网络的鲁棒型哈希方法。

收稿日期：2011-02-22；修回日期：2011-03-04
作者简介：陈青华（1977—），男，山东人，硕士，副教授，从事数字图像处理、模式识别研究。

1 基于 BP 神经网络的鲁棒型图像哈希方法

1.1 BP 神经网络

BP 神经网络又称为反向传播型神经网络，由信息的正向传播和误差的反向传播两个过程组成。BP 神经网络的拓扑结构包括输入层（input layer）、中间层（hide layer）和输出层（output layer）。输入层负责接收来自外界的输入信息，并传递给中间层的各个神经元；中间层负责信息变换，根据信息变化能力的需求，中间层可以设计为单隐层或多隐层结构，最后一个隐层传递到输出层，经进一步处理后，完成一次学习的正向传播处理过程；输出层负责向外界输出信息处理结果。当实际输出与期望输出不符时，进入误差的反向传播阶段。误差通过输出层，按误差梯度下降的方式修正各层权值，并向中间层、输入层逐层反传。而复始的信息正向传播和误差反向传播过程，是各层权值不断调整的过程，也是神经网络学习训练的过程，此过程一直进行到网络输出的误差减少到可以接受的程度，或者预先设定的学习次数为止。BP 神经网络的结构如图 1。

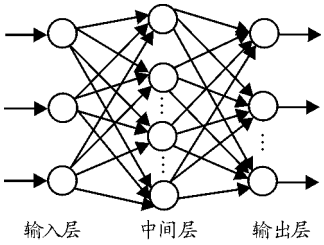

图 1 BP 神经网络的结构

1.2 哈希值产生过程

1) 按式 (1) 构建像素向量 $P_{N\times N}$。

$$p(i,j)=i-1-255\times floor(j/255) \qquad (1)$$

其中，$p(i,j)$ 为像素函数，$1\leqslant i\leqslant N$, $1\leqslant j\leqslant N$; floor(.) 函数的功能是取实数整数部分。

2) 归一化处理。

设灰度图像的像素矩阵为 $\boldsymbol{T}$，其大小为 $N\times N$，分别将矩阵 $\boldsymbol{P}$ 和 $\boldsymbol{T}$ 进行归一化，产生新矩阵 $\boldsymbol{P}$ 和 $\boldsymbol{T}$。

3) 创建并训练 BP 神经网络。

以矩阵 $\boldsymbol{T}$ 为输入层，矩阵 $\boldsymbol{P}$ 为输出层来组建 BP 神经网络。由于输入的样本是整幅图像的数据，而输出的样本是一个一维的序列，因此输入和输出的模式不同，数据相关性相差较大，这就需要在输入层和输出层之间加入中间层，形成数据之间的中间转换，由于处理数据信号的能力是随着层数的增加而增加的，但是过多的隐层又会造成训练时间的急剧增加。使用 2 个隐层来完成 BP 神经网络的训练，第 1 个隐层有 3 个神经元，该层的传递函数采用正切 S 型传递函数；第 2 个隐层有 1 个神经元，该层的传递函数采用对数 S 型传递函数。整个神经网络的训练函数使用了贝叶斯正则化函数，并设置了目标值 0.01 和迭代次数 1 000 次，其结构如图 2。

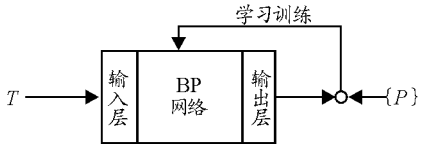

图 2 训练 BP 网络

4) 产生哈希值

对图像矩阵 $\boldsymbol{T}$ 作离散小波变换，产生低频分量 L，其大小为 $N/2\times N/2$，将低频分量组成大小为 $N\times N$ 的矩阵 $\boldsymbol{T}'$，如式 (2)：

$$\boldsymbol{T}'=\begin{bmatrix} L & L \\ L & L \end{bmatrix} \qquad (2)$$

把矩阵 $\boldsymbol{T}'$ 作为输入项，输入到训练好的 BP 网络中，生成哈希值 H，如图 3。

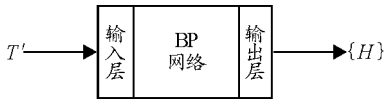

图 3 利用 BP 网络产生哈希值

1.3 图像认证

认证阶段步骤如下：

1) 将接收到的图像 P'，按照哈希值的生成步骤生成哈希值 $H'_{(P')}$。

2) 把 $H'_{(P')}$ 与原图像 P 的哈希值 $H_{(P)}$，记两者不相同位的个数为 $diff$，如式 (3)。

$$diff=\sum_{i=1}^{Len}|H'(i)-H(i)| \qquad (3)$$

其中，Len 为哈希序列的长度。

3) 按式 (4) 对收到的图像进行认证。

$$f(P,P')=\begin{cases}1, & if\ diff/Len<\vartheta \\ 0, & otherwise\end{cases} \qquad (4)$$

其中，$f(.)$ 为图像真实性验证函数；ϑ 为哈希序列差异率阈值。

2 仿真实验

在 Matlab7.0 平台下对算法进行了大量的仿真

实验。实验选用大小为 256×256 的标准 Lena、Baboon 和 Boats 灰度图像作为输入图像。在 BP 神经网络中选取 σ 为 0.01，训练次数为 1 000。

2.1　鲁棒性分析

新算法在高斯噪声、剪切、JPEG 压缩和中值滤波操作下的性能表现如图 4～图 7。

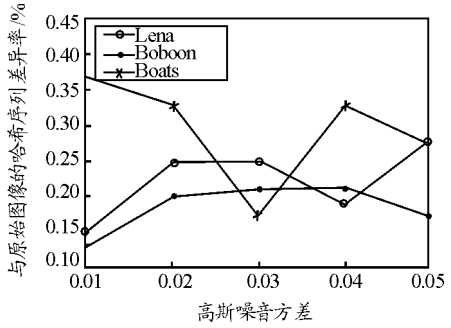

图 4　算法的抗高斯噪声性能

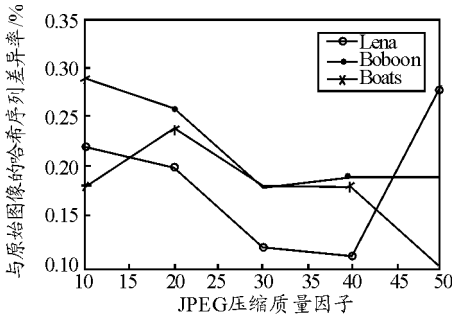

图 5　算法的抗 JPEG 压缩性能

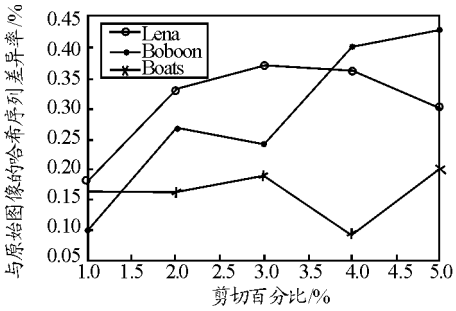

图 6　算法的抗剪切性能

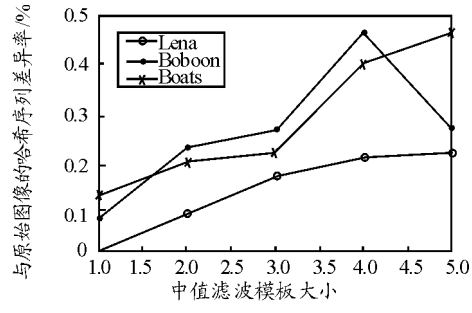

图 7　算法的抗中值滤波性能

图 4 中是设定高斯噪声的均值为 0，在不同的方差的情况下比较本文算法的性能，可以看出大部分的 Hash 值序列距离是在 0.30 以下。图 5 中是在不同的 JPEG 压缩质量因子下对算法进行的比较，可以看出所有的 Hash 值序列距离都在 0.30 以下，即算法对 JPEG 压缩的鲁棒性很好。图 6 中的横坐标为图像的剪切百分比，在仿真的过程是将图像的左上角要剪切的部分像素值设为 0，由于剪切也是对图像的一种损坏，所以随着剪切百分比的增加，图像 Hash 值的距离也随着增加。图 7 是对图像进行中值滤波，在模板大小未超过 3 时，算法的鲁棒性较好。从图 4 中可以看出，该算法具有较好的抵抗高斯噪声、JPEG 压缩、剪切和中值滤波。

2.2　强壮性分析

通过计算 Lena，Baboon 和 Boats 之间的 Hash 值距离来分析算法的强壮性，不同图像之间的标准汉明距离越大，算法强壮性越高，如表 1。

表 1　图像之间的 Hash 距离

图像	Lena	Baboon	Boats
Lena	0.00	0.43	0.31
Baboon	0.43	0.00	0.49
Boats	0.31	0.49	0.00

从表 1 可以看出 3 个图像之间的 Hash 距离基本上都在 0.30 以上，说明新算法具有较好的强壮性。

3　结束语

实验结果表明，基于 BP 神经网络的新型图像 Hash 算法对高斯噪声、JPEG 压缩、中值滤波等操作具有较好的鲁棒性，为图像的版权保护提出了一种新 的途径。如何进一步增强图像的鲁棒性，降低图像冲突的概率，将是下一步的研究工作。

参考文献：

[1] Monga V, Mihcak K M. Robust and secure image hashing via non-negative matrix Factorizations[J]. IEEE Trans. on information forensics and security, 2007, 2(3): 376-390.

[2] 张维克, 孔祥维, 尤新刚. 安全鲁棒的图像感知哈希技术[J]. 东南大学学报: 自然科学版, 2007, 37(1): 188-192.

[3] 邹建成, 周红丽, 邓欢军. 一种安全鲁棒的图像哈希方法[J]. 计算机应用研究, 2009, 26(6): 2122-2124.

[4] 孙锐, 闫晓星, 丁志中. 一种用于图像认证的感知哈希方法[J]. 系统仿真学报, 2010, 22(2): 483-487.