数字水印中 FCM 算法的应用研究

Applying Fuzzy C-means Clustering Algorithm in Digital Watermarking

张 伟

(重庆教育学院计算机与现代教育技术系 重庆400067)

Abstract As an effective method of ownership assertion for digital media, digital watermarking has been targeted especially in recent years. From characteristics, general framework and applications of digital watermarking, we present a new way to insert a fine digital watermarking in an image in this paper. The image is divided into two categories, one is suited for inserting a digital watermarking, the other is not. So, we can select the appropriate pixels in an image to insert the digital watermarking. In the end, we also present results from two image experiments to show that our approach is applicable in practice.

Keywords Digital watermarking, Clustering, Fuzzy C-means clustering

1 引言

多媒体数据的数字化为多媒体信息的存取提供了极大的方便,同时也极大地提高了信息表达的效率和准确性。随着因特网的日益普及,其上的数字媒体(数字声音、文本、图像和视频)应用正在呈爆炸式的增长,越来越多的知识产品以电子版的方式在网上传播。由于数字信号处理和网络传输技术可以对数字媒体的原版进行无限制的任意编辑、修改、拷贝和散布,造成数字媒体的知识版权问题日益突出。因此如何既利用因特网的便利,又能有效保护知识产权,受到了人们的高度重视。数字水印技术作为数字媒体版权保护的有效办法,从1993年 Caronni 正式提出到现在短短的时间里,已经成为多媒体信息安全领域的一个热点。

聚类的目标是将数据聚集成类,使得类间的相似性尽量小,而类内的相似性尽量大。聚类通过比较数据的相似性和差异性,能发现数据的内在特征及分布规律,从而获得对数据更深刻的理解与认识,所以它受到了科技界的广泛关注。本文对数字水印中 FCM 算法的应用进行了研究。

2 数字水印技术

2.1 数字水印的概念

数字水印(digital watermarking)是永久镶嵌在其他数据(宿主数据)中具有可鉴别性的数字信号或模式(如一段文字、标识、序列号或徽标等),而且并不影响宿主数据的可用性。被嵌入的信息通常是不可视或不易察觉的,但是通过一些操作可以被检测或者被提取。

水印与源数据(如图像、音频、视频数据)紧密结合并隐藏其中,成为源数据不可分割的一部分,并可以经历一些不破坏源数据使用价值或商用价值的操作而存活下来。在数字水印系统中,隐藏信息的丢失,即意味着版权信息的丢失,从而也就失去了版权保护的功能,也就是说,这一系统就是失败的。由此可见,数字水印技术必须具有较强的鲁棒性、安全性和透明性。

2.2 数字水印系统模型

下面图1为水印信号插入模型,其功能是将水印信号加入原始数据中;图2为水印信号提取模型,其功能是从水印数据中提取出水印信号;图3为水印信号检测模型,用以判断某一数据中是否含有指定的水印信号。

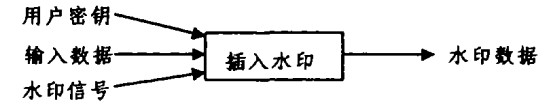

图1 水印插入

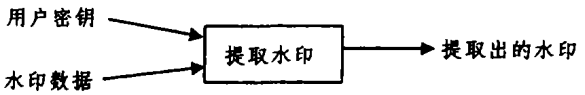

图2 水印提取

图3 水印检测(适用于强壮水印)

2.3 数字水印的应用

(1)维护所有权/指纹(Ownership Assertion/Fingerprinting):谁拥有作品的版权?谁未经授权进行了作品的拷贝?

(2)信息隐藏(Data Hiding or Steganography):将重要信息隐藏起来,使可能的监察者察觉不到有这样一个信息在发送。这与传统密码学有本质的区别。

(3)认证和完整性检测(Authentication and Tamper Detection):可验证数字化内容是否被修改、造假。此类水印必须是脆弱的,且检测时不需要原始数据。

(4)内容标识(Content Labeling):加入的水印信息构成一个注释,提供有关产品内容的进一步信息,如图像的拍摄日期、地点等。

(5)使用控制(Usage Control):加入水印来标识允许的拷贝数。如 DVD 防拷贝系统,每拷贝一份,由硬件修改水印内容,将允许的拷贝数减一,以防止大规模的盗版。

(6)内容保护(Content Protection):加入可见的但难以去除的水印图像,防止用于商业目的。

3 FCM 算法

设有 n 个待聚类样本(或模式),类别个数为 c,特征数为 s,有如下定义:

定义1 样本集 $X=\{x_1,x_2\cdots,x_n\}$是任一有限集，$x\subset R^S$；V_{cn}是 $c\times n$ 阶实矩阵的集合；c 是整数，$2\leqslant c\leqslant n$。则称下述集合为 X 的模糊 C-划分空间：

$$M_{fc}=\{U\in V_{cn}\mid 0\leqslant u_{ik}\leqslant 1,\forall\ i,k;\sum_{i=1}^{c}u_{ik}=1,\forall\ k;0\leqslant\sum_{k=1}^{n}u_{ik}<n,\forall\ i\}$$

式中 u_{ik}是隶属度矩阵 $U\in M_{fc}$的 i 行 k 列元素，表征 x_k 对于类 i 的隶属度值。

定义2 设 $v_i\in R^l$ 是类别 i 的聚类中心矢量。定义 C-聚类中心矩阵为

$$V=(v_1,v_2,\cdots,v_c)\in R^{cl}$$

定义3 模糊 C-均值聚类目标函数 $J_m:M_{fc}\times R^{cl}\to R^+$为

$$J_m(U,V)=\sum_{k=1}^{n}\sum_{i=1}^{c}(u_{ik})^m(d_{ik})^2$$

式中$(d_{ik})^2=\|x_k-v_i\|^2=(x_k-v_i)^T(x_k-v_i)$；$m$ 称为加权指数，$m\in[2,\infty)$。

为得到样本集合 X 的最佳模糊 c 划分，可通过如下的迭代优化算法来使目标函数 $J_m(U,V)$最小：

1)确定聚类数目 c，$2\leqslant c\leqslant n$；确定参数 m，$2\leqslant m<\infty$；

2)确定初始隶属度矩阵 $U^{(0)}=(u_{ik}^{(0)})$；

3)令初始迭代次数 $b=0$；

4)利用下式求各类的聚类中心 $v_i^{(b)}$，$i=1,2,\cdots,c$，

$$v_i=\sum_{k=1}^{n}u_{ik}^m x_k/\sum_{k=1}^{n}u_{ik}$$

5) 按如下方法计算新的隶属度矩阵 $U^{(b+1)}$，对 $k=1$至 n；

计算 I_k 和$\overline{I_k}$：

$$I_k=\{i\mid 1\leqslant i\leqslant c;d_{ik}=\|x_k-v_i\|=0\}$$

$$\overline{I_k}=\{1,2,\cdots,c\}-I_k$$

若 $I_k=\phi$，则

$$u_{ik}=1/\sum_{j=1}^{c}(d_{ik}/d_{jk})^{2/(m-1)}$$

否则，对所有 $i\in\overline{I_k}$，置 $u_{ik}=0$，并取

$$\sum_{i\in I_k}u_{ik}=1,k=k+1$$

6) 选用适宜的矩阵范数比较 $U^{(b)}$和 $U^{(b+1)}$：若$\|U^{(b)}-U^{(b+1)}\|<\varepsilon$，停止；否则令 $b=b+1$，返回4)。ε 是收敛阈值。

4 FCM 具体应用

图像作为一种数字媒体，选择图像中适合嵌入水印的位置(或像素点)是值得研究的课题。在水印嵌入方案中，基本遵循的原则是最大限度地利用人类视觉系统 HVS(Human Visual System)模型。其基本思想是利用从视觉模型导出的 JND(Just Noticeable Distortion)描述来确定在图像的各个部分所能容忍的数字水印信号的最大强度，从而避免破坏视觉质量。我们采用的手段是应用 HVS 模型，并结合 FCM 算法，将图像划分为两个类：一个类适合于嵌入数字水印，有较强的透明性和鲁棒性，水印更隐蔽，不宜觉察；另一个类则不适合于嵌入数字水印。

设像素(i,j)周围3×3邻域为 $N(i,j)$。为了对图像的局部特征进行模糊聚类，我们依据人类视觉模型(HVS)和相关统计知识，考察如下五个特征(我们在原有四个特征基础上，增加了梯度敏感值一个特征)：

(1)亮度敏感值，即灰度均值，代表子图的亮度。

$$B=\frac{1}{9}\sum_{N(i,j)}g_{ij}$$

(2)梯度敏感值，即梯度模，用于衡量图像在所有方向变化的敏感度。

$$G=\frac{1}{9}\sum_{k=-1}^{1}\sum_{t=-1}^{1}|g_{i+k,j+t}-g_{ij}|\ (k\text{ 和 }t\text{ 不同时为零})$$

(3)纹理敏感值，即灰度的方差，决定子图的纹理。

$$T=\sum_{N(i,j)}|g_{ij}-B|$$

(4)对比度敏感值，即灰度之间的最大距离，表现为子图对比度。

$$C=\max(g_{ij})-\min(g_{ij})$$

(5)熵敏感值，即信息论中的熵计算式，用于对子图的不确定性进行度量。

$$E=-\sum_{N(i,j)}p_{ij}\cdot\log p_{ij}$$

其中 g_{ij}表示像素(i,j)的灰度值，P_{ij}定义如下

$$P_{ij}=g_{ij}/\sum_{N(i,j)}g_{ij}$$

这样每个像素点就对应了五个值，它们构成了一个特征向量：$X(B,G,T,C,E)$

因此，可以将整幅图像的所有像素点看作是五维空间上的一个元素，对它们应用 FCM 算法，就能够把图像分为两个类：一个类适合于嵌入数字水印，而另一个类则不适合于嵌入数字水印。

5 实验结果

对图像 Baboon(256 * 256)和 Lena(256 * 256)分别进行了计算机仿真实验，结果如下：

表1 图像 Baboo 聚类中心计算结果

聚类中心	亮度敏感值	梯度敏感值	纹理敏感值	对比度敏感值	熵敏感值
v1	135.5374	103.0732	88.0941	38.3947	2.1890
v2	121.8639	334.2298	261.6799	102.7239	2.1482

表2 图像 Lena 聚类中心计算结果

聚类中心	亮度敏感值	梯度敏感值	纹理敏感值	对比度敏感值	熵敏感值
v1	125.7247	39.3056	38.8513	14.3155	2.1951
v2	107.9211	189.8379	185.9970	69.3819	2.1631

敏感值越大，表明该类更能容忍视觉上的误差，也就是说适合嵌入水印。于是从表1和表2得知，v2类适合于嵌入数字水印，v1类则不适合。使用一定的阈值 T0对隶属度矩阵进行划分，相应地得到如图(b)(c)所示的分类图。图中亮色区域为v1，较适合于嵌入数字水印。适当地增大分割阈值，可得到范围稍小些的 v1类。

(a) (b) (c)

图4 (a)Baboon 原图 (b)阈值 T0=0.55时的分类图 (c)阈值 T0=0.90时的分类图

(下转第133页)

和B模型相比，还增加了自己的新特点，即主体的权限扩大。在原有的B模型中为了实现数据的保密性，禁止任何形式的向下写，高级主体不能向低级客体中写任何信息，包括非高级客体中的信息。而在三层B模型中，主体通过对中间体的执行，可实现部分的下写。比如现在有高级别主体s，低级别进程im(中间体)，和与im同级别的客体文件o_1，o_2。进程im的功能是从文件o_1读取信息然后把信息写入文件o_2。那么主体s对im的执行最终导致的结果是向低级别文件中写入了同级别的信息，这种对数据的写入不会造成任何高级信息的下漏。所以说我们的三层B模型是在保持数据保密性的前提下对B模型的改进，扩充了B模型中主体的权限，即高级别主体可以向低级别客体中写入低级别的信息，所以这个模型更具有实用性。改进示意图如图2。

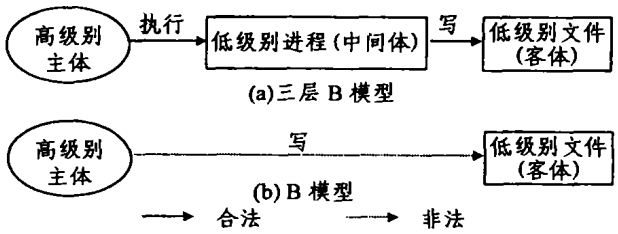

图2　三层B模型和B模型比较图

4. 三层B模型的应用展望

因为三层B模型具有的新特点，将使得它在数据库，操作系统的设计中有着广泛的使用前景。这个模型尤其适合使用在操作系统的设计中，在操作系统的设计中，用户将承担主体的角色，进程将承担中间体的角色，而各种文件将是客体。用户对于进程的读写将成为进程对于输出设备的输出和获得输入设备的数据，而进程对于文件的读写则是一般概念上的读写，用户对于进程的执行也是一般概念上的执行。中间体的数目随着进程的创建，结束而变化。于是整个对于客体文件的读写都由作为中间体的进程完成，主体用户要对客体文件进行读写操作时，都必须通过运行相应进程(如果用户运行一个执行文件，那么他运行后产生的进程的级别就是这个执行文件的级别)，由进程把读到的信息输出给主体用户(即输出到输出设备上)，这样完成主体用户的读；用户把输入信息输入到输入设备中，再由进程读取，这样完成主体用户的写。当低级别的主体用户需要把信息写入低级别的客体文件时，他可以把这个权限赋予给高级别的主体用户，即编写相应写入文件进程(这个进程必须没有对输入输出设备的读写)，把该进程交给高级别主体用户执行，这样就完成了高级别主体用户向低级别客体文件写入信息的过程，值得我们注意的是，这时高级别主体写入的内容是低级别的内容而不是高级别客体中的内容，所以没有造成高级别信息的泄漏。同时当高级别的主体用户需要把高级别主体文件中的信息写入同级别的客体文件时，他也可以编写一个读写进程(该进程也不能有对输入输出设备的读写，否则低级别的客体用户就不能运行)交给低级别的主体用户执行。

当然，这个模型也会有自己不完善的地方，它应用于操作系统可能还需要改进，但是对于大多数基于B模型的操作系统来说，将其建立成基于三层B模型的操作系统，将是一件非常有意义的事情。

参考文献

1 Bell D E, La Padula L J. Secure Computer System: Mathematical Foundations. The Mitre Corp, Bedford, Mass: [Tech Rep MTR-2547]. Vol I, 1973

2 Bell D E, La Padula L J. Secure Computer System: a Mathematical Model. The Mitre Corp, Bedford, Mass: [Tech Rep MTR-2547]. Vol II, 1973

3 Bell D E, La Padula L J. Secure Computer System: a Refinement of the Mathematical Model. The Mitre Corp, Bedford, Mass: [Tech Rep MTR-2547]. Vol III, 1973

4 Sandhu R S. Lattice-based access control models. Computer, 1993,26(11):9～19

5 Biba K J. Integrity Considerations for Secure Computer Systems, The Mitre Corporation, Bedford, MA, April 1977

6 洪帆，蔡蔚，余详宣. 一个用于多级安全关系数据库系统的改进Bell-La Padula模型. 计算机学报，1995,18(10):763～769

7 杨智慧. 计算机信息系统安全技术. 北京：群众出版社，1998

(上接第118页)

(a)　(b)　(c)

图5　(a)Lena原图　(b)阈值T0=0.35时的分类图
(c)阈值T0=0.60时的分类图

隶属度值U的大小还可以作为该点嵌入水印强度系数，以实现自适应水印嵌入。具体应用FCM聚类算法的数字水印方案，我们将在后续工作中予以报道。

参考文献

1 Cox I J, Killian J, Leighton T, Shamoon T. Secure spread spectrum watermarking for images, audio and video. In: Pro. IEEE ICIP (Int. Conf. on Image Processing), Lausane, Switzerland, 1996. 243～246

2 Hsu C-T, Wu J-L. Hidder signature in images. In: Proc of ICIP, 1996. 223～226

3 O'Ruanaidh J, Pun T. Rotation, scale and translation invariant spread spectrum digital image watermarking [J]. Signal Processing, 1998, 66(3): 303～317

4 Der-Chyuan LOU, Te-Lung YIN. Adaptive digital watermarking using fuzzy clustering technique. IEICE trans. fundamentals, 2001, E84-A(8)

5 Jain A K, Dubes R C. Algorithms for Clustering Data. Prentice Hall, 1988

6 Murty M N, Jain A K. Knowledge-based Clustering Schema for Collection Management and Retrieval of Library Books. Pattern Recognition, 1995, 28(7)

7 Shortland R, Scarfe R. Digging for Gold (Data Management). IEE Review, 1995, 41 (5): 213～217

8 Han J. Conference tutorial notes: Data Mining Techniques. In: Proc. of ACM SIGMOD Intl. Conference' 96 on Management of Data (SIGMOD' 96). Montreal, Canada, June 1996