基于混沌加密和零树编码的彩色图像水印算法

杨蒙召,李朝峰,许 磊
(江南大学 信息工程学院,江苏 无锡 214122)

摘 要:为了保证水印嵌入具有速度快、易实现的优点,并且提高其安全性和鲁棒性,文中利用混沌系统的优良特性,首先对一个有意义二值图像进行快速混沌加密,然后依据零数编码思想对小波系数按重要性排序,选取最重要的 L 个系数作为水印的嵌入点,即对人类视觉最重要的部分,在其位平面内嵌入加密过的水印,最后反变换得到嵌入水印后的载体图像。试验证明,该算法具有效率高、抗压缩能力强、较好的鲁棒性等优点。

关键词:水印;混沌系统;零树编码思想
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2006)10-0157-03

A Color Image Watermarking Algorithm Based on Chaotic Encryption and Zerotrees Coding Idea

YANG Meng-zhao, LI Chao-feng, XU Lei
(School of Information Technology, Southern Yangtze University, Wuxi 214122, China)

Abstract: In order to insure the watermarking embedding merits, such as high speed, easy realization, etc. and improve its safeness and robustness, a meaning binary image is encrypted quickly based on chaos theory because of chaos system merits. Then the wavelet coefficients are arrayed by their importance and the most important number L coefficients, the part which is most important to the human vision, is selected as the spot which should be embedded by watermarking. At last the watermarking is embedded in the coefficient bit plane and the carrier image containing the watermarking is acquired by the retransform. The experimental result proves that this algorithm has merits such as high efficiency, strong ability to resist compression, better robustness, etc.

Key words: watermarking; chaos system; zerotrees coding idea

0 引 言

数字水印是一种嵌入到图像、视频或音频中的不可见数据,用于对信息数据的版权进行注册、认证或保护,具有很广泛的应用领域。现有的图像水印算法基本上可分为两类:空间域方法和变换域方法。空间域方法通过直接改变某些变换系数来加入水印,而变换域方法先对图像作某种变换,例如离散余弦变换(DCT)、离散小波变换(DWT),然后通过改变某些变换系数来加入水印。变换域的优点是:

①嵌入的信号能量可分布到空间的所有像素上,有利于保证水印的不可见性;

②变换域中,可以更方便地将人类视觉系统(HVS)的某些特性结合到水印算法中;

③变换域方法可以与现有的图像压缩方法兼容,从而实现压缩图像的水印嵌入。

鉴于变换域方法的诸多优点,目前很多数字水印算法都采用小波变换和其它模型方法结合起来用于数字水印的嵌入、提取和检测,例如基于HVS模型、奇异值分解、复数小波变换、基于混沌理论置乱加密等等[1~5]。其中将混沌理论的非线性技术引入到数字水印算法中[6],是近年来提出的一个比较好的思想,这已经被国内外诸多论文证实了采用混沌理论的科学性和有效性。

随着网络带宽的增加和人们视觉上的需要,彩色图像越来越普遍地被人们传播和使用,出于安全考虑,研究彩色图像数字水印变得非常实用和有价值。文中结合混沌理论和零树编码思想提出了一个彩色图像数字水印算法。其基本思想是:零数编码[7]是一个成熟的图像压缩方法,但是这里利用它构造零树过程的思想,对小波系数进行重要性排序,取最重要的 L 个系数作为水印的嵌入点,即对人类视觉最重要的部分,在其位平面内嵌入混沌加密过的水印,这就保证了原有算法按照从幅度大的小波系数到幅度小的小波系数、低频系数多高频系数相对少,这样一个合理次序嵌入水印,使所选择的小波系数更加合理地覆盖了小波系数的低频和高频部分,相对拓宽了覆盖范围,并且在图像的重要部分嵌入了较多的水印,从而具有较好的鲁棒性。

收稿日期:2005-12-07
作者简介:杨蒙召(1980-),男,河南鲁山人,硕士研究生,研究方向为模式识别与图像处理;李朝峰,副教授,硕士生导师,研究方向为人工智能与模式识别。

1 混沌水印的产生

混沌现象是在非线性动力系统中出现的类似随机的过程,这种过程既非周期又不收敛。一个离散时间混沌系统的定义如下[8]:

$$X_{n+1} = f(X_n) \quad -1 < X_n < 1;\ n = 0,1,2,\cdots \tag{1}$$

式中 X_n 表示系统状态,f 为当前状态 X_n 到下一状态 X_{n+1} 的映射。若以初值 X_0 开始迭代,所得序列 $\{X_n \mid n = 0,1,2,\cdots\}$ 就称为该离散时间动力系统的一条轨道。运用于产生伪随机序列的离散混沌映射较多,最常用的有:

Logistic 映射:

$$x_{n+1} = \mu x_n(1 - x_n) \quad -1 \leqslant x_n \leqslant 1 \tag{2}$$

Chebyshev 映射:

$$x_{n+1} = \cos(\mu \arccos x_n) \quad -1 \leqslant x_n \leqslant 1 \tag{3}$$

如对于Logistic映射,当 μ 从0变化到3.156 994 5时,该动力系统则因从稳定状态到分叉而产生倍周期,当 3.156 994 5 $< \mu \leqslant 4$ 时,该动力系统进入混沌状态。当 $\mu = 4$ 时,这两个映射都处于混沌状态,都能产生混沌序列,其 Lyapunov 指数分别为 ln2 和 1.387 8,说明在初始条件 x_0 稍微出现一个偏差 D_{x_0} 时,采用 Chebyshev 映射,经过 n 次迭代后的误差 $D^n_{x_0}$ 相对小,于是在对水印信号加密时采用 Chebyshev 映射。

混沌函数具有伸大拉长、折回重叠、随机遍历的性质,所以有不可预测性,混沌序列的产生和复制很方便,只要给出一个混沌迭代公式和一个初值,就能产生一个混沌序列,通过改变混沌系统参数及初始值还可以得到数量巨大的序列,并且序列长度是任意的。因此,研究基于混沌的数字水印信号的设计,将有利于数字水印的标准化,进而推动数字水印技术走向实用。

这里设 W 为 $N_1 \times N_2$ 的水印图像,采用 Chebyshev 映射产生一个混沌序列 $\{x_i \mid i = 1,2,\cdots,L\}$,其中 $L = N_1 * N_2$,将实数值序列量化为二进制位序列 $\mid x \mid = b_1(x)b_2(x)\cdots b_i(x)\cdots$,都选取第 k 位作为编码位,这样就得到了一个二值序列 $\{b_k(x_i) \mid i = 1,2,\cdots,L\}$,加密过的水印图像为:$W^* = W(i) \oplus b_k(x_i)$,$\oplus$ 为异或操作。这里将密钥定为 k 和 X_0,如果不知道此密钥,也就无法得到近似原始 W 的水印图像了。

2 水印嵌入算法

文中假定使用 $M \times M$ 大小的真彩色图像,所选最大的小波系数 L 个,水印嵌入算法如下:

(1) 读取 $M \times M$ 大小的原始真彩色图像 X,将它从 RGB 空间转换到 YIQ 空间中,选取 Y 分量,进行 3 级小波变换得到其 1 个低频部分和 9 个高频部分,在小波变换后得到的所有小波系数中选取最大的小波系数 L 个:$\mathrm{Max}_i(i = 1,2,\cdots,L)$。

(2) 将系数 Max_i 乘以 10^n 后取整操作,将取整后的 Max_i 转化为二进制的字符串形式,并求出相应的二进制位的长度 length,通过下面的公式计算出水印的嵌入位:

$$v = \max(^L(\mathrm{length}(\min a) + \mathrm{length}(\mathrm{mean}) + \mathrm{length}(\max a))/6,6) \tag{4}$$

其中 min a,max a,mean 是矩阵 ca3 的系数取绝对值后,P 个最小值、最大值及整个矩阵的均值乘上 10^n 取整后转化为二进制位串的值,其目的是为了消除图像处理和攻击对个别系数的影响,在文中 P 取 100。length 为求字符串长度函数,max 为求最大值函数,$^L()$ 为向下取整函数。

(3) 通过位操作将第 v 位(从左至右计算,即从高位至低位,以下同)的二进制位修改为与水印位相同,$v+1$ 位置 1,其余的 length $- v - 1$ 位置 0,算法如下:

```
for(i = 1,…,L)
  if(W(i) = = 1)
    Max_i(v) = 1;
  else
    Max_i(v) = 0;
  end
end
Max_i(v + 1) = 1;
for(k = (v + 2):length)
    Max_i(k) = 0
end
```

(4) 将修改后的二进制位串转化为十进制的整数,并除以 10^n 得到嵌入水印后的系数 Max_i^*。

(5) 将修改后的 $\mathrm{Max}_i^*(i = 1,2,\cdots,L)$ 覆盖原来的 Max_i,然后进行小波逆变换,最后将逆变换得到的图像从 YIQ 空间转换到 RGB 空间,即得到最后的含有数字水印的彩色图像 X^*。

3 水印提取算法

水印的提取算法是嵌入算法的一个逆过程,其大致步骤描述如下:

(1) 读入含有数字水印的彩色图像 X^*,将其由 RGB 空间转换到 YIQ 色彩空间,并提取出 Y 分量进行 3 级小波变换,选取变换后最大的小波系数 L 个:$\mathrm{Max}_i^*(i = 1,2,\cdots,L)$。

(2) 将系数 Max_i^* 乘上一个 10^n,并做取整操作,将取整后的 Max_i^* 转化为二进制的字符串形式,并求出相应的二进制位的长度 length,通过公式(4) 计算出水印的提取位 v'。

(3) 通过位操作,判断系数第 v' 位的奇偶性,得到相应的水印位信息。

(4) 通过循环操作,重复执行上述步骤 L 次,得到水印信息 W^*。

(5) 再根据密钥,即可得到近似于 W 的水印图像 W^*。

4　试验结果

(1)客观评价指标。

为了更加科学地分析文中算法嵌入和提取水印图像的效果，这里定义了 2 个客观评价参数，公式如下：

① 峰值信噪比(PSNR)：

$$PSNR = 20\log_{10}\left(\frac{255}{RMSE}\right)$$

$$RMSE = \sqrt{||W^{**} - W||^2/M*N} \qquad (5)$$

其中：W^{**}，W 分别是提取出的水印和原始水印，M，N 分别为图像的行数和列数，255 是图像中像素点的最大像素值。PSNR 越高，说明文中算法嵌入和提取的水印的效果越好。

② 在水印的检测中，为了描述提取出来的水印图像 W^{**} 和原始水印图像 W 的相似程度，定义相似度系数：

$$\rho(W, W^{**}) = \sum_{i=1}^{L} W(i)W^{**}(i) \Big/ \left(\sqrt{\sum_{i=1}^{L} W(i)^2}\sqrt{\sum_{i=1}^{L} W^{**}(i)^2}\right) \qquad (6)$$

显然 ρ 越接近 1 越好。

(2) 试验结果及分析。

文中采用了 Matlab 进行仿真试验，自制水印为标有江南大学英文简称“SYTU”32 × 32 的二值图像(如图 1 所示)，混沌加密后的水印如图 2 所示。选取真彩色图像 Lena 为载体图像如图 3(左) 所示，通过算法分析和多次试验结果表明：$n = 3$，$v = 6$ 时效果较好，采用 db1 小波对载体图像进行 3 层小波变换，依据上面所叙述的算法，得到的含水印的载体图像如图 3(右) 所示。

图 1　二值图像　图 2　混沌加密后的水印

图 3　原始载体图像和含水印载体图像

①水印抗噪声检测：对图 3 含水印的载体图像加入椒盐噪声，然后依据水印提取算法从含噪声图像中提取水印，两幅图像如图 4 所示。这里得到的提取出来的水印和原始水印的峰值信噪比与相似度分别为：PSNR = 28.063 7，ρ = 0.905 0，从中可以看出虽然载体图像含有较多的噪声，但该算法依然可以提取出易识别的水印信息。

②水印抗剪切性检测：对图 3 含水印的载体图像进行约 31% 的剪切，然后从中提取出来水印，这两幅图像如图 5 所示。这里得到的提取出来的水印和原始水印的峰值信噪比与相似度分别为：PSNR = 26.362 1，ρ = 0.887 3，从峰值信噪比、相似度和直观上都可以看出效果不如水印抗噪声检测的图像结果，但还是仍旧可以识别出水印信息。

图 4　含噪声载体图像和所提取水印图像

图 5　剪切 31% 的载体图像和所提取水印图像

③水印抗压缩检测：对图 3 中含水印的载体图像，采用 JPEG 标准进行压缩，然后从中提取出来水印，两幅图像如图 6 所示。这里得到的提取出来的水印和原始水印的峰值信噪比与相似度分别为：PSNR = 28.972 4，ρ = 0.963 1。从峰值信噪比、相似度和直观上都可以看出，本算法对水印抗压缩效果最好。限于篇幅，本算法对其他方面，诸如水印抗滤波、抗缩放、抗旋转等，不再一一赘述。

图 6　JPEG 压缩后的载体图像和所提取水印图像

5　结　论

阐述了一种基于混沌加密和零树编码的彩色图像水印算法，从实验结果看，该算法的优点是：

①由于引入了具有诸多优点的混沌动力系统，故可使该水印算法具有更好的鲁棒性和安全性；

②采用零树编码的思想选取的嵌入点，低频部分嵌入多和高频系数嵌入相对少，较均匀地覆盖所有的小波系数，所以更具有合理性；

③由于是对较少的水印信息先加密，所以计算效率

(下转第 162 页)

in)已存在的处理好的降维空间中[8]。前一种方法,重新计算 SVD 要花费很多的时间和很大的内存要求,但是,它直接影响后面得到的潜在语义结构;后一种方法则是以已存在的结构为基础,需要时间少、内存小,但新加进来的词、文档,对先前的词、文档表示没有太大影响。对于新文档 D 添加到降维空间,可以由按表达式(6)处理方法推导出来其在降维空间的表示:

$$d = D^{T}TS^{-1} \tag{8}$$

同理,也可以将新加入的词向量 W 看作是 $1 \times n$ 的词向量,可以通过下面的推导得到其在降维空间中的向量表示 w:

$$W = wS_kD_k^{T} \Rightarrow (WD_kS_k^{-1} = wS_kD_k^{T}(D_kS_k^{-1}) \Rightarrow w = WD_kS_k^{-1} \tag{9}$$

2 讨 论

这种方法,首先应用到信息检索是以 Deerwester 为首的 Bellcore 研究组,他们开发出了 LSI 及其升级版 LSI + + 系统[5,9]。这种方法可以解决词语的共现问题,查询语义的模糊性;能够真正地表示和覆盖初始语义结构;SVD 更加简洁、紧凑;但是,这种方法要进行高维的矩阵相乘,不能够表示 Inverted Index,对每一个单一的文档计算查询 - 文档相似性要比 Inverted Index 慢,同时,在计算"词 - 文档"矩阵时,不能直接用词的计数,而是要对其进行权重的计算,后进行标准化。

在实际的应用中,特别是对中文的处理,LSI 模型比较适合对大的查询输入进行查询,而对一些短的查询输入效果就没有大的查询输入好了,因为这时候在查询的语句中,每个词可能只出现一次,因此从查询向量自身看不出哪个词重要,哪个词不重要。通过国外对西文的处理的借鉴,研究者们提出了一种改进思路:使用 pseudo relevance feedback(或 pseudo - feedback, two - stage retrieval)技术作为对 LSI 的改进。这种思路就是先用 LSI 进行一次查询返回一个结果,再在这些返回的文档中选取和查询句子相似度最高的 N 篇,后将其主要的关键词抽取出来,再添加到查询向量中去,现假定已取定相关文档向量 d 则由 1.3 节的式(6)可得到新的查询向量的表示:

$$q = Q^{T}T_kS_k^{-1} + d^{T}D_k \tag{10}$$

这样,就用相关文档的关联词扩充了查询向量,使查询得到更好的效果。就现在来看,对西文的处理是比较好的,但是由于中文的特殊性,处理起来效果如何还有待于验证。

参考文献:

[1] Chien Lee - Feng, Pu Hsiao - Tieh. Important Issues on Chinese Information Retrieval Computational Linguistics and Chinese Language Processing, 1996, 1(1):205 - 221.

[2] 邹 涛,王继成,张福炎.基于 WWW 的资料搜集系统的设计与实现[J].情报学报,1999,18(3):195 - 201.

[3] Chien Lee - Feng. PAT - Tree - Based Keyword Extraction for Chinese Information Retrieval[J]. SIGIR, 1997, 31(SI): 50 - 58.

[4] Deerwester S, Dumais S T, Furnas G W, et al. Indxing by latent semantic analysis[J]. Journal of the American Society for Information Science, 1990, 41(6):391 - 407.

[5] Letsche T A, Berry M W. Large - Scale Information Retrieval with Latent Semantic Indexing [J]. Information Science, 1997, 100(1):105 - 137.

[6] 史忠植.知识发现[M].北京:清华大学出版社,2002.

[7] Manning C D, Schutze H. Foundations of Statistical Natural Language Processing [M]. Cambridge, Massachusetts: The MIT Press, 1999.

[8] Berry M W, Dumais S T, O'Brien G W. Using linear algebra for intelligent information retrieval[J]. SIAM Review, 1995, 37(4):573 - 595.

[9] Husbands P, Simon H, Ding C. On the Use of Singular Value Decomposition for Text Retrieval[A]. 1st SIAM Computational Information Retrieval Workshop[C]. Raleigh, NC:[s. n.], 2000.

(上接第 159 页)

高,因此本算法是一种可行的、比较实用的算法。

另外本算法也不是完美的,比如对水印的抗剪切性能不是很好,还有待于进一步改进和完善。

参考文献:

[1] Delaigle J F, Vleeschouwer C D, Macq B. Watermarking algorithm based on a human visual model[J]. Signal Proc, 1998, 46(5):319 - 336.

[2] 宋 琪,吴林东,朱光喜.一种基于 HVS 的利用零树编码的水印算法[J].华中科技大学学报(自然科学版),2004,32(5):5 - 7.

[3] 王琛晖,舒志彪.一种基于小波变换和人类视觉系统的自适应水印算法[J].福州大学学报(自然科学版),2004,32(12):50 - 54.

[4] 高仕龙.基于复小波变换和奇异值分解的数字水印[J].乐山师范学院学报,2004,12:5 - 8.

[5] 陈鹤峰.基于图像置乱与重复嵌入的鲁棒水印技术[J].计算机应用,2005,25(2):412 - 413.

[6] 欧珊瑚,张 珩.基于混沌特性和视觉模型的小波数字水印算法研究[J].中国图象图形学报,2004,9(3):345 - 351.

[7] Shapiro J M. Embedded image coding using zerotrees of wavelet coefficients[J]. IEEE Trans on Signal Proc, 1993, 41(12):3445 - 3462.

[8] 吕金虎.混沌时间序列分析与应用[M].武汉:武汉大学出版社,2002.