

基于喷泉码的数字图像水印的研究

张卫党, 李方圆, 陈美玲

(郑州大学 信息工程学院, 河南 郑州 450001)

摘要: 为了提高数字图像水印信息传输过程中的鲁棒性, 这里提出一种基于喷泉码的数字水印算法, 该方案利用喷泉码在删除信道中的优异性能, 将信道编码与扩频水印结合后在图像中嵌入水印信息. 然后对这种方案在水印系统中的鲁棒性进行了一系列仿真测试, 并与未编码方案及水印系统中常用到的 LDPC 编码方案作了比较. 仿真证明, 应用该方案可以提高数字水印系统的鲁棒性, 降低水印信息在传输过程中的误码率, 而且水印编码复杂度要远远低于 LDPC 方案.

关键词: 数字水印; 喷泉码; 鲁棒性

中图分类号: TP309.2 **文献标志码:** A **doi:**10.3969/j.issn.1671-6833.2014.06.013

0 引言

数字水印技术目前已成为多媒体信息安全研究领域发展最快的热点技术之一. 数字水印算法主要分为空间域和变换域两大类^[1]. 空间域算法实现简单, 能满足水印的不可见性要求, 但其鲁棒性较差; 相比于空间域水印算法, 变换域算法对常见图像处理和压缩更有鲁棒性, 但缺点是水印嵌入量较小, 计算复杂. 数字水印系统与通信系统之间存在着相似性, 为了进一步提高水印信息在传输过程中的抗干扰能力, 增强其鲁棒性, 很多研究者将信道编码技术引入到数字水印系统中作为水印信息的预编码, 并和一些成熟的水印算法结合, 取得了不错效果. 文献[2]将线性分组码引入到水印系统中取得了一定的效果; 文献[3]中将 CDMA 扩频水印与 Turbo 码结合在 DCT 和 DWT 混合变换域中嵌入水印提高了水印的安全性和鲁棒性; 文献[4]利用 LDPC 码的纠错性能和人眼视觉特性实现了图像的水印嵌入和提取.

Michael Luby 在 1998 年提出了用于删除信道的喷泉码 (fountain code) 的概念, 并于 2002 年提出了第一种实用的喷泉码——LT 码^[5]. LT 码是一种性能很好的纠删码, 其编码速率动态可变, 适用于删除概率未知的信道, 因其编译码方法简单且复杂度低, 故具有很好的应用前景^[6].

笔者基于以上考虑, 将文献[7]中用到的基于双伪随机序列的扩频水印与 LT 编码相结合提

出一种新的数字水印算法. 该算法以变换域中 DCT 变换为基础, 结合符合人眼视觉特性的 HVS 视觉模型^[8], 利用 LT 码良好的纠删性能, 在水印检测过程中将不能正常判定的信息删除, 利用能判定出的信息恢复出水印. 笔者研究了该方案在水印传输过程中的鲁棒性, 并与水印系统中纠错性能很好的 LDPC 码的性能作了对比分析.

1 水印的生成算法

本文的水印生成算法将基于双伪随机序列扩频水印与 LT 编码结合来产生待嵌入的水印信息, 原始水印可采用一副二值图像以减少待嵌入信息的数据量. 水印图像首先转换成一维二进制序列 $\mathbf{m} = [m_1, m_2, \dots, m_k]^T$, 然后进行 LT 编码. 具体 LT 码的编译码方案及 LT 码的性能参考文献[9]和[10]. 设定 LT 编码后的信息长度为 N , 并构造出生成矩阵 \mathbf{G} , 得到编码后的信息序列. 设编码后信息为单极性二值序列, 即

$$\mathbf{m}' = \{m'_i \mid m'_i \in \{0, 1\}, 0 \leq i \leq N-1\}. \quad (1)$$

然后采用基于双伪随机序列的扩频方法生成扩频水印, 设要生成待嵌入的水印序列长度为 $N \cdot R$. 首先由密钥 S 产生两个长度为 R 的独立二值伪随机序列如下:

$$\begin{cases} \mathbf{p}_0 = \{p_{0j} \mid p_{0j} \in \{1, -1\}, 0 \leq j \leq R-1\}; \\ \mathbf{p}_1 = \{p_{1j} \mid p_{1j} \in \{1, -1\}, 0 \leq j \leq R-1\}. \end{cases} \quad (2)$$

最终生成的待嵌入的水印序列可描述如下:

收稿日期:2014-06-07; 修订日期:2014-09-09

基金项目:国家自然科学基金委员会-中国民用航空总局联合研究基金项目(U1204607)

作者简介:张卫党(1958-), 男, 河南郑州人, 郑州大学教授, 博士, 主要从事信道编码研究, E-mail:iewdzhang@zzu.edu.cn.

$$\mathbf{w} = \left\{ w_k \mid w_k = \begin{cases} p_{0j}, m_i = 0 \\ p_{1j}, m_i = 1 \end{cases} \right\}, \quad (3)$$

其中, $i = \left\lceil \frac{k}{R} \right\rceil, j = k \bmod(R), 0 \leq k \leq N \cdot R - 1$.

2 水印的嵌入算法

水印的嵌入算法采用基于 DCT 域 HVS 视觉模型,为平衡不可见性与抗攻击性,将图像进行 8×8 分块后选择在子块 DCT 域的中频区域嵌入水印,这里修改待嵌入子块的 22 个中频系数来嵌入水印. 水印嵌入算法采用加法规则,如式(4)表示

$$I_w(x, y) = I(x, y) + \alpha \cdot w(x, y). \quad (4)$$

式中: α 为嵌入强度; $I(x, y)$ 、 $I_w(x, y)$ 分别为图像嵌入水印前后的 DCT 系数; $w(x, y)$ 为由密钥 S 生成的伪随机序列扩频而得的待嵌入序列. 这样就可把待嵌入的信息嵌入到图像的指定位置.

3 水印的提取

对待测图像进行水印提取时,首先对待测图像进行 8×8 分块 DCT 变换,取出每个子块的 22 个中频系数,通过密钥 S 生成与嵌入时相同的两组独立的伪随机序列 p_1 和 p_0 ,计算伪随机序列与提取出的子块的中频系数的相关值. 相关值的计算式子如(5)所示, $I'_w(i)$ 为第 i 块提取出的 22 个中频系数,其中 $\overline{I'_w(i)}, \overline{p_1}, \overline{p_0}$ 分别为 $I'_w(i), p_1, p_0$ 的均值.

$$\left\{ \begin{aligned} \delta_1(i) &= \frac{\sum_{j=1}^{22} (I'_w(i, j) - \overline{I'_w(i)}) (p_1(j) - \overline{p_1})}{\sqrt{\sum_{j=1}^{22} (I'_w(i, j) - \overline{I'_w(i)})^2} \sqrt{\sum_{j=1}^{22} (p_1(j) - \overline{p_1})^2}}; \\ \delta_0(i) &= \frac{\sum_{j=1}^{22} (I'_w(i, j) - \overline{I'_w(i)}) (p_0(j) - \overline{p_0})}{\sqrt{\sum_{j=1}^{22} (I'_w(i, j) - \overline{I'_w(i)})^2} \sqrt{\sum_{j=1}^{22} (p_0(j) - \overline{p_0})^2}}. \end{aligned} \right. \quad (5)$$

相关值反映了提取出的中频系数与嵌入的信息的相关程度,它的取值在 $[-1, +1]$ 之间,如果该值超过某一阈值,就可以判定图像中该子块含有水印信息. 此处设定两个阈值 z_1 和 z_0 ,提取公式如下:

$$\begin{cases} \text{if } \delta_1(i) > \delta_0(i) \text{ and } |\delta_1(i)| > z_1, w'(i) = 1; \\ \text{if } \delta_0(i) > \delta_1(i) \text{ and } |\delta_0(i)| > z_0, w'(i) = 0. \end{cases} \quad (6)$$

否则,视为该处未提取出水印信息,并把 LT 编码的生成矩阵 G 中的相应列删除. 阈值的设定由实验得出. 本文中取 $z_1 = \overline{|\delta_1|}, z_0 = \overline{|\delta_0|}, \overline{|\delta_1|}, \overline{|\delta_0|}$ 分别为 N 个子块中的中频系数与 p_1, p_0 相关值的绝对值的平均值. 由提取出的信息及更新过

的生成矩阵 G 进行 LT 译码即可恢复出水印序列 m'' .

4 所提方案性能分析

仿真测试中,原始载体图像采用 512×512 的 lena 灰度图像,水印采用 32×32 的二值图像. 图 1 为原始载体图像和 LT 编码方案的含水印图像;图 2 为二值水印图像.



(a) Lena 原始图像 (b) 含水印图像
图 1 lena 原始载体图像和含水印图像
Fig. 1 Original image and watermarked image

copy

图 2 二值图像水印

Fig. 2 Watermark

因嵌入强度大小与水印的抗攻击性有关,嵌入强度越小抗攻击性越差,反之,不可见性又会受到影响. 为了平衡抗攻击性和不可见性的关系,实验采用的嵌入强度 $\alpha = 15$,图 1(b) 的峰值信噪比 (PSNR) 为 31.99 dB. 本实验中原始载体图像可划分为 4 096 个 8×8 的子块,3 种方案均采用双伪随机序列扩频方法, LDPC 编码方案采用码率为 1/4, LLR BP 译码算法且最大迭代次数为 100 次的非规则 LDPC 码,其校验矩阵的列重为 3,行重不固定. LT 编码方案和 LDPC 编码方案均将原始水印编码成 4 096 bit 待嵌入信息嵌入到载体图像的每一块中,未编码方案的水印信息嵌入到原始图像方差最高的前 1 024 块. 表 1 是 3 种方案在未攻击情况下提取出的水印图像及误码率 (BER).

表 1 未攻击情况下提取出的水印图像及 BER

Tab. 1 The BER and recovered watermark under no attack

方案	图像水印	BER/%
未编码	copy	0.781 3
LDPC 编码	copy	0.488 3
LT 编码	copy	0

4.1 抗 JPEG 压缩性能

图 3 为 JPEG 压缩品质因数 Q 与提取出来的水印误码率之间的关系图. 图像压缩 Q 的取值为 $0 \sim 100$, Q 值越大表明压缩越少,图像质量越高.

由图 3 可以看出,当 Q 值大于 40 时,应用 LT 编码方案能够无差错地将水印信息提取出来,性

能优于未编码及 LDPC 编码方案;当 $Q=30$ 时,LT 编码方案性能低于 LDPC 方案,这是由于当 Q 过低时,图像出现严重失真,水印检测过程中能正确提取出来的信息不足以让 LT 码进行完全译码,所以使恢复出的水印的误码率变大.

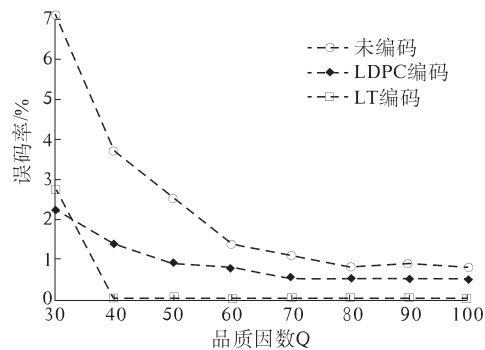


图 3 JPEG 压缩下的 BER 性能
Fig.3 The BER under JPEG attack

4.2 抗剪切性能

表 2 中给出了不同剪切比例下 3 种方案的抗剪切性能.其剪切位置为含水印图像的左上角.可

表 2 不同剪切比例下提取出的水印及 BER
Tab.2 The BER and recovered watermark caused by crop attack

方案	剪切比 25%		剪切比 50%		剪切比 65%	
	水印	BER/%	水印	BER/%	水印	BER/%
未编码		13.671 9		41.406 3		55.273 4
LDPC 编码		0.488 3		0.488 3		12.402 3
LT 编码		0		0		0

表 3 中值滤波提取的水印及 BER
Tab.3 The BER and recovered watermark caused by Median filtering attack

方案	窗宽 1		窗宽 2		窗宽 3	
	水印	BER/%	水印	BER/%	水印	BER/%
未编码		0.781 3		12.402 3		16.015 6
LDPC 编码		0.488 3		8.496 1		5.273 4
LT 编码		0		0		1.562 5

4.4 抗噪性能

在含水印图像中加入不同类型的噪声干扰会引起水印的部分丢失.为了验证本文所提方案对噪声攻击下的鲁棒性,实验采用方差为 0.005 和 0.5 的高斯白噪声和密度为 0.01 和 0.1 的椒盐噪声分别对含水印图像进行攻击,表 4 中为两种类型的噪声攻击下提取出的水印信息的 BER,其中高斯白噪声攻击实验的 BER 是进行了 100 次的平均值.

从表 4 可以看出,对于高斯噪声攻击,当噪声方差小时 LT 编码方案的 BER 低于未编码方案;

以看出,加入信道编码后的方案要比未编码时的抗剪切性好的多.因为 LT 码在删除信道中的性能优异,在剪切攻击中,被剪切掉的子块中含有的水印信息提取不出来而被删除,而剩余的子块中则可以正确提取出嵌入的信息,只要提取出来的信息个数能够使 LT 码译码成功就可以无失真恢复出水印图像.在 LT 编码方案中,若要译码成功,就必须提取出足够的信息使其进行译码,也就是说如果剪切比例太大,提取不出足够的信息进行 LT 译码,就会使 BER 急剧增加,例如,本实验中若剪切比例为 70%,经验证,此时提取出的水印信息的误码率为 71.191 4%.

4.3 抗中值滤波性能

对图像进行中值滤波是用来减少高频噪声,而往图像中添加水印相当于引入噪声,故含水印图像在中值滤波后会产生失真.含水印图像经过不同窗宽的中值滤波后提取水印的 BER 如表 3 所示.由表 3 可以看出,在抵抗中值滤波攻击中,LT 编码方案的误码率更低,所体现的性能更佳.

而当噪声方差较大时,LT 编码方案的 BER 甚至高于未编码方案,这是由于在噪声方差过大时,图像污染严重,在水印信息检测时,LT 编码方案提取出了大量错误信息,再进行译码时因其不具备纠错功能,故使恢复出的水印的误码率增大.

对于椒盐噪声,由表 4 可知,在噪声密度较小时,LT 编码方案中可以将加噪的子块完全区别出来,故可以完全恢复出水印图像,优于另外两种方案.而当噪声密度过大时,误码率升高的很快.因此,LT 编码方案对弱噪声攻击有一定的抵抗性,其在强噪声攻击下的性能还有待提高.

表 4 高斯噪声椒盐噪声引起的 BER
Tab.4 The BER caused by Gaussian noise
or pepper and salt noise %

方案	高斯噪声		椒盐噪声	
	0.005	0.5	0.01	0.1
未编码	5.631	11.020	2.343 8	16.210 9
LDPC 编码	3.828	16.370	2.050 8	15.625 0
LT 编码	3.830	21.990	0	25.000 0

笔者还对 3 种方案的水印嵌入时间作了一个对比,水印嵌入实验均仿真 100 次,取 100 次嵌入时间的平均值,未编码、LDPC 编码和 LT 编码方案下平均水印嵌入时间分别为 1.69 s、334.4 s 和 121.8 s. 加 LDPC 编码方案的水印嵌入时间要远远大于未编码方案,而加 LT 编码方案水印嵌入时间虽然也较未编码方案长,但比 LDPC 编码方案要短很多. 由于 LT 编码方案对水印信息鲁棒性的提高有很好的效果,综合考虑认为该方案是可行的算法.

5 结束语

利用双伪随机序列扩频水印方法将 LT 码引入到了数字水印系统中,对数字水印中常见攻击下的鲁棒性有了较好的改善,因其编译码复杂度比 LDPC 码简单的多,故在数字水印系统中 LT 方案比 LDPC 方案实现起来简单. 为了进一步更好地改善抗攻击性,今后可将 LT 码与传统的纠错码结合,尽可能降低水印信息在传输过程中的误码率,更好地提高数字水印系统的鲁棒性.

参考文献:

[1] 尹浩,林闯,邱锋等. 数字水印技术综述[J]. 计算机

研究与发展,2005,42(7):1093 – 1099.
[2] CHEN Yong-cong, CHANG Long-wen. A secure and robust digital watermarking technique by the block cipher RC6 and secure hash algorithm[C]//Proceedings of 2001 IEEE, International conference on Image Processing. Thessaloniki, Greece; IEEE Rress, 2001: 518 – 521.
[3] 许文丽,李磊,王育民. 抗噪声、几何失真和 JPEG 压缩攻击的鲁棒数字水印方案[J]. 电子与信息学报, 2008,30(4):933 – 936.
[4] 霍智勇,朱秀昌. 基于 LDPC 码的数字图像水印技术研究[J]. 中国图像图形学报,2007,12(11): 2018 – 2025.
[5] MICHAEL L. LT Codes [C]// Proceedings of the 43rd Annual IEEE Symposium on the Foundations of Computer Science. Vancouver B C, Canada; IEEE Press, 2002:271 – 280.
[6] 慕建君,焦晓鹏. 数字喷泉码及其应用的研究进展与展望[J]. 电子学报,2009,37(7):1571 – 1577.
[7] MORA-JIMENEZ I, NAVIA-VAZQUEZ A. A new spread spectrum watermarking method with self-synchronization capabilities[C]//Proceedings of 2000 IEEE, International Conference on Image Processing. Vancouver BC, Canada; IEEE Press, 2000:415 – 418.
[8] 易开祥. 数字图像加密与数字水印技术研究[D]. 杭州:浙江大学信息工程学院,2001.
[9] DAVID J C M. Fountain codes[J]. IEEE Communications Proceedings,2005,152(6):1062 – 1068.
[10] SHOKROLLAHI A. Raptor codes[J]. IEEE Transactions on Information Theory, 2006, 52(6): 2551 – 2567.

Study of Digital Image Watermarking Based on Fountain Code

ZHANG Wei-dang, LI Fang-yuan, CHEN Mei-ling

(School of Information Engineering, Zhengzhou University, Zhengzhou 450001, China)

Abstract: This paper presents a new algorithm based on fountain code to improve robustness of the watermark in digital image watermarking system. Employing the outstanding performance of LT codes in erasure channel, the proposed scheme combines channel coding with spread spectrum watermarking to recover watermark. In the end, this paper makes a series of tests with fountain coding scheme and LDPC coding scheme and non coding scheme, the result shows the scheme proposed in this paper can raise robustness of the digital watermarking system, lower the bit error rate (BER) between watermark and recovered watermark effectively. In addition, fountain coding scheme has lower complexity compared with LDPC coding scheme.

Key words: digital image watermark; fountain code; robustness