使用频域LSB水印算法的鲁棒性分析

胡 东，刘晓云

(电子科技大学自动化学院 成都 610054)

【摘要】对在频域中使用最不显著分量(LSB)算法进行了分析，提出了增强LSB算法鲁棒性的条件和频域LSB的两种定义，并据其构造了具有鲁棒性的LSB算法。为保证水印顽健性，对图像做8×8分块，把各个块的中、低频部分的LSB部分用水印代替，水印的平均强度为被取代部分平均强度的20倍。仿真实验证明：算法在一定条件下，可以具有相当强的鲁棒性。同时，可以提供攻击的合法性辨别和攻击位置确定，并在两个位置提供认证接口，符合水印发展趋势。

关 键 词 最不显著分量; 人眼视觉系统; 数字水印; 鲁棒性
中图分类号 TP309.7 文献标识码 A

Robust Analysis for Using LSB Arithmetic to Embed Watermark in Frequency Domain

HU Dong，LIU Xiao-yun

(School of Automation Engineering, Univ. of Electron. Sci. & Tech. of China Chengdu 610054)

Abstract Under the analysis of LSB arithmetic in frequency domain, this paper presents the situations for enhancing robustness of LSB arithmetic and two definitions for LSB in frequency domain. Based on the first definition, this paper constructs a LSB arithmetic with robust. The original image is disparted into 8×8 blocks, and the LSB of middle and low frequency is displaced with the watermark with the 20 times intension of the replaced part's.The experiments prove that the arithmetic has strong robustness under the given situations.

Key words LSB; HVS; digital watermark; robustness

数字水印是一种可以在开放的网络环境中保护版权和认证来源及完整性的新技术。所谓数字水印即是向欲被保护的多媒体数据嵌入某种信息(即水印)，保护所有者权益跟踪非法拷贝等。按攻击的敏感性来分，数字水印分为顽健性水印和脆弱性水印。脆弱性水印的基本算法之一是最不显著分量(Leat Significant Bits，LSB)算法。当前，水印的发展方向是脆弱性水印和鲁棒性水印相结合，本文提出离散余弦变换(Discrete Cosine Transform，DCT)域LSB分量的两种定义，并基于定义构建水印系统。

1 LSB算法的基本原理

LSB算法的基本原理是：对空域的LSB做替换，用来替换LSB的序列就是需要加入的水印信息、水印的数字摘要或者由水印生成的伪随机序列。由于水印信息嵌入的位置是LSB，为了满足水印的不可见性，允许嵌入的水印强度不可能太高。然而针对空域的各种处理，如游程编码前的预处理，会对不显著分量进行一定的压缩，所以LSB算法对这些操作很敏感。因此LSB算法最初是用于脆弱性水印的。

文献[1]提出了第1个水印模型，它把$N\times M$大小的原始图像Z分解为n个8×8块$Z_i(1\leq i\leq n)$，把Z_i的LSB部分置零，对各个块做数字摘要。同时把作为水印的logo图像A变换为$N\times M$，进行同样的分块，数字摘要和A_i对应异或，得到嵌入水印的数字摘要。然后对它用私钥加密，结果嵌入到相应块的LSB部分。检验过程要用到A，并且用户得到的图像有任何的改变，水印都不可能检测出来。

由于联合摄影专家组(Joint Photographic Experts Group，JPEG)是一种常用的图像压缩算法，当把这种处理看成是合法时，文献[2]对LSB算法做了改进，提出了抵抗JPEG的半脆弱水印系统。该系统基于公钥密码系统和hash函数特点，能反映彩色图像在红色(R)、蓝色(B)、绿色(G)层的哪部分受到攻击。RGB图像在B部

收稿日期：2004 - 07 - 29
作者简介：胡 东(1981 -)，男，硕士生，主要从事数字水印、模式识别方面的研究.

分对应的频率响应最低，所以把原始图像分为R、G、B三部分，对于R、G的LSB部分用一个公钥密码系统以外的密钥(简称k_1)加密，再和原始水印W作XOR运算，得到的M用公钥密码系统加密，得到E。同时把B部分的LSB部分清零。最后，把E加入到B的LSB部分。

2 相关知识

2.1 人眼视觉系统特性及以往的鲁棒性水印经验

人眼视觉系统(Human Visual System，HVS)的特性：(1) 人眼对中等灰度最敏感，向低灰度和高灰度两个方向非线性下降；(2) 人眼对图像平滑区的噪声敏感，对纹理区的噪声不敏感；(3) 边缘信息对于人眼非常重要，必须保证边缘的质量不受大的损害。以往的鲁棒性水印经验是：(1) 水印信息应嵌入在中、低频分量上；(2) 水印应具备相当强度。

根据上述特性，要使嵌入水印后的图像不受到明显的损坏，并且水印保持鲁棒性，应该对图像分块，选择纹理比较复杂的块(需要对所有块分析，以便在保证嵌入的块的数目的前提下，确定选块的门限)；水印嵌入到各个块的中、低频分量上；水印的位置选取考虑对图像边缘的影响。

对图像的纹理信息的评判是复杂的，在本文的方法中，用欧拉数大于1去除平滑区域，再计算不为零的高频分量的个数来确定块的纹理复杂度(一般高频分量越丰富，图像的纹理越复杂[3])。

2.2 LSB定义

定义 1　由于频域系数有正有负，所以频域中定义的LSB分量为：$|a_i|<|\sigma_j|$，其中σ_j是DCT系数分块中除a_i外的系数，$1\le i\le 8$，$a_i\ne 0$。

由于LSB算法是一种替换算法，会对时域图像产生一定的影响。根据DCT变换的逆变换公式：

$$\boldsymbol{A}_{m,n}=\sum\sum a_p a_q \boldsymbol{B}_{p,q}\cos\left[\pi(2m+1)p/2M\right]\cos\left[\pi(2n+1)q/2N\right]\quad m=0,1,\cdots,M-1;\quad n=0,1,\cdots,N-1 \tag{1}$$

式中　$\boldsymbol{A}_{m,n}$为重建的图像矩阵；$\boldsymbol{B}_{p,q}$为DCT系数矩阵；M、N为块的大小。

可以看出，$\cos\left[\pi(2m+1)p/2M\right]\cos\left[\pi(2n+1)q/2N\right]$的值决定了DCT系数对重建图像的每一个像素的影响，而且它的值在[1,−1]间变化。

提高水印鲁棒性的一个有效方法就是增强水印强度，为了不觉察图像的改变，就需要考虑图像边缘，从而提出下面的定义。

定义 2　选择LSB的条件为使得式(2)对图像边缘影响最小的(p,q)对：

$$\sum_{m=1}^{M}\sum_{n=1}^{N}\cos\left[\pi(2m+1)p/2M\right]\cos\left[\pi(2n+1)q/2N\right]\qquad m=0,1,\cdots,M-1;\quad n=0,1,\cdots,N-1 \tag{2}$$

3 应用定义1的水印系统

3.1 水印的生成

本文的水印系统是对选定的8×8块嵌入相同的水印。由于受每个块的中、低频分量数目的限制，水印选为8位的序列。这要求对原始水印做数字摘要(当把块分为n个一组时，可以嵌入$n\times 8$的水印序列)。初始水印可以是图像的序列号、图像特征值和简单的随机序列。在实验中，采用随机序列，但每一幅图像应该拥有自己的水印，且最好是和分发图像的时间标记联系在一起。这样带来的好处是，即使同一幅图像，在不同时间传输，其水印嵌入位置也不同。数字摘要后的水印序列为，$w=[w_1,w_2,\cdots w_8]$。

3.2 水印嵌入过程

3.2.1 图像分块

把图像分成8×8块，对各个块做DCT变换和掩膜运算，找出中、低频中的LSB分量，记录下位置矩阵$\boldsymbol{L}$，计算LSB分量的平均值。对各个块计算Euler数，根据HVS的特点，排除数值为1的块。又由于为0的系数会使计算平均值受到Matlab的精度的影响。因此，选择的块至少应该在做掩膜运算后还包含10个以上的非零系数，并且LSB分量的平均值大于水印平均值的0.01倍。这样，就得到将嵌入水印的块。

3.2.2 水印嵌入

在计算待嵌入水印的平均值时嵌入的水印平均强度调整为各个块的LSB的平均值的20倍，并取代原来的

LSB部分。各个块逆DCT变换，得到水印图像。需要对水印序列和LSB做同向排序，然后对应嵌入，以得到好的视觉效果。最后，把位置矩阵$\boldsymbol{L}$和待嵌入水印w，连同水印图像，一起传输给购买者。

3.2.3 水印检测

用户根据得到的位置信息$\boldsymbol{L}$和原始水印，从$\boldsymbol{L}$指定的位置提取水印。在水印的检测中，可以得到各个块中的水印信息，设得到的水印序列为$s\{i\}$，得到的最终水印序列w为：

$$w(k)=(\sum_{i=1}^{N}s\{i\}(k))/N \qquad k=1,2,\cdots,m \tag{3}$$

式中 m为水印序列包含的位数；$s\{i\}$为第i个嵌入水印的块检测出的水印序列；N为嵌入水印的块的个数。当计算得到序列的平均值处于–0.35±0.05的范围内，说明水印存在。由得到的水印序列，可以看出对图像所做的一些处理，从而知道这种处理的合法性。同时，这种分析可以精确到块。

4 水印的抗欺骗性

水印的欺骗是指，攻击者替换图像中的水印，导致认证失效。攻击者在不能解密$\boldsymbol{L}$的情况下，得到$\boldsymbol{L}$，是这种攻击的前提。由前边的水印嵌入检测过程和对水印强度的操作，使得水印超出了原来的LSB部分的数值范围。由于平均值是统计特性，各个水印元素还有差异，这进一步增大了数值范围，导致攻击者要完成欺骗攻击，必须平均对各个块做2.558 6×10^9次运算才能找到水印的位置信息。而这个方法的前提必须是攻击者得到合法购买的图像，且攻击的结果只是得到自己这幅图像的水印位置。又由于每幅图像嵌入的水印不同，使得攻击得到的水印位置信息，对于其他图片的破解是没有意义的。

5 实验结果

实验采用的是名为“lena”的bmp图像，大小为320×320。水印序列为[–0.2，–0.2，–0.3，–0.3，–0.4，–0.4，–0.5，–0.5]，m=8，共有1 600个块。“lena”实际嵌入的是118个块，N=118。图1是嵌入水印前后的对比；图2是对数变换实验结果；图3是JPEG的实验结果。

a. 原始图像

b. 水印图像

图1 嵌入水印前后对比

图2 对数变换实验结果

a. 品质因子75

b. 品质因子60

c. 品质因子40

图3 JPEG压缩实验

JPEG压缩实验检测出的水印为：(1) [–0.2，–0.3，–0.4，–0.3，–0.3，–0.5，–0.5，–0.5]；(2) [–0.3，0，–0.6，–0.4，–0.4，–0.4，–0.6，–0.5]；(3) [0，0，0，–0.3，–0.7，–0.6，–0.5，–0.4]。

原始水印的平均值为–0.35，实验检测出的平均值分别为–0.35、–0.31、–0.31、–0.36、–0.4、–0.31。用平均值作为检测标准时，正负0.05都为水印存在的范围。

图2是对数变换实验结果，检测出的水印为[–0.2，–0.2，–0.3，–0.3，–0.3，–0.3，–0.4，–0.4]。对于对数变换，由于其本质是降低图像的灰度差。从结果中也可以清楚地看到，嵌入到初始强度最大位上的水印强度降低了。所以在门限相同的情况下，对数变换和JPEG改变的水印位置是不同的。

对于图像质量的变化，可采用多人辨别方法。经过6个人对图1的观察，在嵌入强度为20时，水印图像和原始图像没有差别。

6 结 束 语

本文设计的水印系统，结合了鲁棒性水印和脆弱性水印的优点，在±0.05的检测范围内，对多种攻击均可检测到水印。且可以判断攻击发生的位置，以及其中几种攻击的类型。同时，在水印嵌入位置***L***和原始水印摘要的传输中，可采用公钥体制来保证安全。当符合定义2时，嵌入强度可以达到30，但可嵌入水印的块会减少。

本文的研究工作得到了电子科技大学青年科技基金(YF021405)的资助，在此表示感谢！

参 考 文 献

[1] WONG P W. A watermark for image integrity and ownership verification[J]. Proc、Int、Conf、Image Processing, 1997, 1: 680-683.
[2] BYUN S C, LEE I L, SHIN T H, et al. A public-key based watermarking for color image authentication[C]// IEEE, Korea, 2002: 593-596.
[3] 黄继武, SHI Y Q, 姚若河. 基于块分类的自适应图像水印算法[J]. 中国图像图形学报, 1998, 4(A)(8): 460-463.

编　辑　漆　蓉

(上接第735页)

在不同BER情况下，自适应FEC都能以较少的冗余数据获得较高的接收效率，固定FEC虽然在某个BER下可能表现出较好的性能，但当BER改变时则缺少相应的应变能力。

为了验证自适应FEC在BER动态变化时的性能，在发送数据过程中改变链路的BER测试了各个FEC的效能。每次发送有效数据均为3 000 kbytes。

在动态变化中，BER在0.000 75与0.000 15之间来回跳变，每发送500个Packet跳变一次。图4中P_a表示平均*PER*，*n*表示已发送的Packet个数。可以看到自适应FEC的平均*PER*明显优于FEC_1和FEC_2，与FEC_3则非常贴近。由于计算的是收到所有包的平均*PER*，累积了前面的丢包过程，所以曲线的波动幅度逐渐减小，但仍可看出P_b变化时*PER*的波动过程。FEC_3的冗余数据量始终为5.8%，自适应FEC在这里的冗余数据比例为4.1%，可见自适应FEC能尽量用较少的开销得到较多的收益。

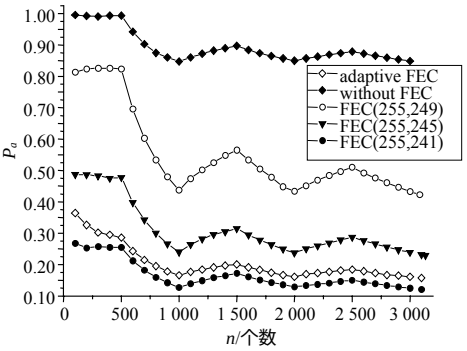

图4　各FEC在BER作动态变化时平均PER曲线图

4 结 束 语

本文提出了一种应用于Ad hoc网络的基于主动网的自适应FEC协议，用以改善无线信道BER突发多变的状况。通过仿真实验进行了性能分析和比较，其结果表明，基于主动网的自适应FEC可有效降低无线信道中的PER，并能根据实际链路状况尽量减少冗余负担，增加带宽的利用率，为无线传输性能的改进提供了一种有效的手段。

参 考 文 献

[1] 王　斌. 主动式网络及应用关键技术研究[D]. 西安: 西安电子科技大学, 2001.
[2] 赵志峰, 郑少仁. Ad hoc网络体系结构研究[J]. 电信科学, 2001, 17(1): 14-17.
[3] Miyoshi M, Sugano M, Murata M. Performance improvement of TCP on wireless cellular networks by adaptive FEC combined with explicit loss notification[C]//Vehicular Technology Conference IEEE, Birminghan, 2002, 55(2): 982-986.
[4] Ayanoglu E, Paul S, LaPorta T F, et al. AIRMAIL:A link-layer protocol for wireless networks[J]. Wireless Networks,1995, 1(1):47-60.
[5] Eckhardt D A, Steenkiste P. A trace-based evaluation of adaptive error correction for a wireless local area network[J]. Mobile Networks and Applications, 1999, 4(4): 273-287.
[6] Liu Benyuan, Goeckel D L, Towsley D. TCP-cognizant adaptive forward error correction in wireless networks[C]// Global Telecommunications Conference GLOBECOM IEEE, Taipei, 2002, 02: 2128-2132.
[7] Lemmon J J. Wireless link statistical bit error model[EB/OL]. http://its.bldrdoc.gov/pub/ntia-rpt/, 2002-06-16.

编　辑　孙晓丹