

# 一种鲁棒性好的图像水印算法\*

尹康康, 石教英, 潘志庚

(浙江大学 CAD&CG 国家重点实验室, 浙江 杭州 310027)

E-mail: jyshi@cad.zju.edu.cn

http://www.zju.edu.cn

**摘要:** 提出了一种鲁棒性好的数字图像水印算法. 算法采用 Hilbert 扫描顺序, 用考虑 HVS (human visual system) 特性的噪声阈值矩阵作为叠加水印信号的掩模插入水印, 并具有水印强度自适应调节特性. 水印检测算法还可加入自动校正模块, 大大提高了判决的准确性. 在描述算法的基础上, 给出了实验结果及攻击分析. 实验结果表明, 该算法具有较强的透明性和鲁棒性, 水印检测结果准确, 并且算法的计处量小.

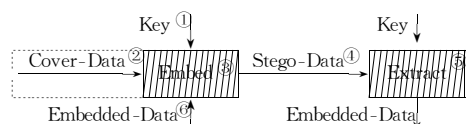
**关键词:** 信息隐藏; 数字水印; Hilbert 扫描; 人类视觉系统; 攻击分析

中图法分类号: TP391

文献标识码: A

信息隐藏 (steganography 或 information hiding) 主要研究如何将一个信息隐藏起来, 致使可能的监察者甚至不知道有这样一个信息在发送, 而密码学中的监察者是知道有一个秘密信息在发送的, 这是信息隐藏与传统密码学的一个本质不同. 这就像一个人可以用奇怪的文字书写他要发送的信息, 也可以用看不见的墨水书写他要发送的信息一样.

如图 1 所示是在第 1 界国际信息隐藏学术研讨会上达成的关于信息隐藏核心系统的模型及其



①密钥, ②原始数据, ③嵌入, ④隐密数据, ⑤提取, ⑥隐藏信息.

Fig. 1 Reference model of core components in stegosystem

图1 信息隐藏核心系统参考模型

相关术语<sup>[1]</sup>. 其中数据类型可以是“文本”、“消息”、“图像”、“声音”等合适的数据类型. 隐藏信息代表被隐藏的内容. 原始数据是隐藏内容的原始载体, 可以从外界输入, 也可以在隐藏过程中产生. 隐密数据是隐藏过程的输出, 是载有隐藏信息的数据. 密钥是在隐藏过程中需

要的密钥, 在提取隐藏消息的过程中通常也需要此密钥.

信息隐藏作为一门新兴学科, 以如何隐藏一个消息的存在为其研究内容, 在计算机、通信、保密学及信号处理等领域有着广阔的应用前景. 它在计算机多媒体技术领域的一个重要应用就是数字水印技术.

数字水印 (digital watermarking) 技术, 是指在数字化的数据内容中嵌入不明显的记号. 被嵌入的记号通常是不可见或不可察的, 但是通过一些计算操作可以被检测或者被提取出来. 水印与源数据 (如图像、音频、视频数据) 紧密结合并隐藏其中, 成为源数据不可分离的一部分, 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.

\* 收稿日期: 1999-09-27; 修改日期: 2000-03-07

基金项目: 国家自然科学基金资助项目 (60033010; 60083009); 浙江省自然科学基金资助项目 (RC00048)

作者简介: 尹康康 (1974—), 女, 江苏徐州人, 硕士生, 主要研究领域为多媒体, 计算机图形学; 石教英 (1937—), 男, 浙江宁波人, 教授, 博士生导师, 主要研究领域为多媒体, 虚拟现实技术, 科学计算可视化; 潘志庚 (1965—), 男, 江苏淮安人, 博士, 研究员, 博士生导师, 主要研究领域为多媒体, 分布式图形, 虚拟现实技术.

根据信息隐藏的目的和技术要求,数字水印具有以下基本特性:(1) 透明性(隐藏性);(2) 鲁棒性;(3) 隐藏位置的安全性.

目前的数字水印算法主要分为:空域/时域算法、频域算法、压缩域算法、基于统计学的算法、利用人类感官生理模型的算法等<sup>[2~7]</sup>. 应用领域主要分为所有权验证、拷贝追踪、完整性验证、标记与注释、使用控制、内容保护等<sup>[8,9]</sup>. 有关具体内容可参考文献<sup>[10]</sup>.

本文提出的数字水印算法属于空域水印算法,同时利用了人类视觉系统的特性. 空域算法中具有代表性的是 Hartung 算法<sup>[3]</sup>和 Kankanhalli 算法<sup>[7]</sup>. 其中 Hartung 算法没有引入人类视觉系统的特性,透明性较差. Kankanhalli 算法在 Hartung 算法的基础上利用了人类视觉系统特性,但是可感知噪声阈值矩阵在 DCT(discrete cosine transform)频域内计算,大大增加了空域水印算法的计算开销. 另外,水印叠加采用光栅扫描顺序进行,求和窗口内像素相关性差;局部水印强弱不均,无自适应调节能力;对受到几何形变攻击的水印图像,水印检测算法无法作出正确判定. 本文提出的算法很好地解决了 Hartung 算法和 Kankanhalli 算法中存在的这些缺陷.

本文第 1 节是水印算法描述,第 2 节给出相关实验及攻击分析,第 3 节对算法进行总结和讨论.

1 鲁棒性好的图像水印算法

1.1 Hilbert 扫描

Hilbert 扫描是一种空间填充曲线<sup>[11]</sup>. 通常在将二维图像序列转化为一维序列时采用光栅扫描,即行或列的连接. 它的缺陷是只利用了二维图像中一个方向的相关性. Hilbert 扫描可以很好地保留二维相关性. 如图 2 所示为 3 阶 Hilbert 曲线的示意图,可以看出,这种扫描的盘旋结构将图像中具有高相关性的数据汇集到了一起. 对于  $2^n \times 2^n$  的图像,我们可以递归地构造  $n$  阶的 Hilbert 曲线<sup>[12]</sup>. 我们给出两个抽象的递归函数  $[i, j] = \text{Hilbert2Matrix}(t, n)$  和  $[t] = \text{Matrix2Hilbert}(i, j, n)$ , 进行一维 Hilbert 曲线中某个像素点的下标  $t$  与其在图像矩阵表示法中的下标  $(i, j)$  的相互转化,其中  $n$  是 Hilbert 曲线的阶. 还可将 Hilbert 曲线推广到任意大小的网格上<sup>[13]</sup>,使得其应用更加具有灵活性.

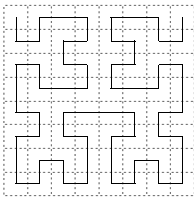


Fig. 2 The third order Hilbert curve  
图2 3阶Hilbert曲线

1.2 水印嵌入算法

算法的基本框图如图 3 所示. 为了算法描述简单,采用 256 级的灰度图像作为原始图像. 算法的基本思想是将水印信号的比特流转化成类似于噪声的信号加入图像中,即对每个像素点的灰度值作轻微扰动,使其携带水印信息. 考虑到透明性和鲁棒性的要求,算法引入了一系列增强性能的机制,包括基于人类视觉系统(human visual system,简称 HVS)特性的噪声分配、位扩展、用伪随机序列<sup>[14]</sup>调制水印信息、采用 Hilbert 扫描.

在图 3 中,  $I(i, j) \{1 \leq i \leq n, 1 \leq j \leq n\}$  代表原始图像中第  $i$  行第  $j$  列像素的灰度值.  $J(i, j)$  是考虑人眼视觉特性而计算出的  $(i, j)$  点的可感知噪声阈值矩阵 JND(just noticeable distortion, 或称为恰可察觉失真矩阵),可以认为,对  $I(i, j)$  引入的噪声信号只要在  $J(i, j)$  这个阈值以下,就不会被人类视觉系统所察觉.

我们的阈值计算主要利用了 HVS 的 3 个特性<sup>[7]</sup>: (1) 人眼对不同的灰度具有不同的敏感性,

通常对中等灰度最为敏感,向低灰度和高灰度两个方向非线性下降;(2)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。

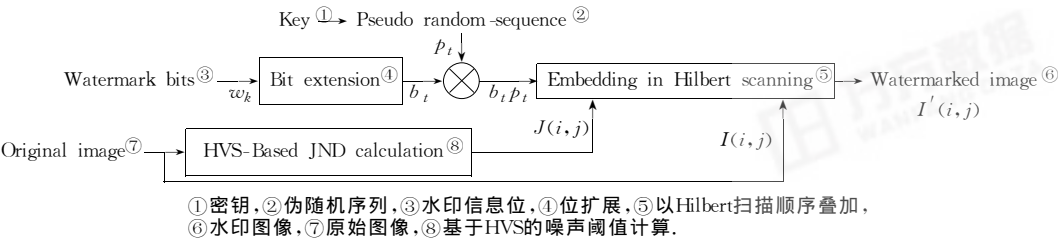


Fig. 3 Watermarking algorithm illustration  
图3 水印算法示意图

具体计算  $J(i, j)$  如下. 首先将图像分成  $8 \times 8$  的小块, 计算每一块的熵值和方差, 熵值较小的块应该是平滑区域, 而熵值较大的区域可能是纹理或边缘, 纹理对应的方差较小, 边缘对应的方差较大. 这样, 我们根据计算将所有的图像块分成 8 类, 为每一类指定一个基准的噪声阈值, 然后对每个像素点根据它的灰度值计算一个与灰度相关的附加噪声阈值, 这个值加上该像素所在小图像块的基准噪声阈值, 就形成了像素  $I(i, j)$  的可感知噪声阈值  $J(i, j)$ . 图像块的数量、图像块分类参数及阈值指派是根据实验确定出的经验值. 一般来说, 要取得最优的  $J(i, j)$ , 这些参数应该根据所选定的原始图像来确定, 但也可以为简化起见, 对不同复杂度的图像给出一组代表值. 细节丰富的图像复杂度高, 平滑的图像复杂度低.

需要指出的是, 文献[4, 7]中的算法也考虑了 HVS 特性来叠加水印, 但这些算法是在频域上计算 JND, 复杂度高, 实时性差. 我们的 HVS 模型形式简单, 可以在空域内直接计算, 计算量较小, 具有较强的使用价值. 我们也可以利用更复杂的 HVS 模型来计算噪声阈值矩阵, 但是, 随着模型的精确化, 算法复杂度也大大提高, 难以保证阈值矩阵计算过程的实时性, 这将影响数字水印系统的处理效率.

下面说明水印算法流程.

设水印信息比特流为  $w_k \in \{0, 1\}$ , 先由一个扩展因子  $cr$  (chiprate) 进行位扩展.

$$b_t = \begin{cases} 1 & w_k = 1 \\ -1 & w_k = 0 \end{cases}, \quad k \cdot cr \leq t < (k+1) \cdot cr. \tag{1}$$

位扩展<sup>[3]</sup>的目的是提供一定程度的信息冗余, 即一个比特的水印信息  $w_k$  由  $cr$  个比特的  $b_t$  序列携带, 冗余度由  $cr$  控制. 冗余度越大, 水印抗攻击的能力就越强, 但同时嵌入水印信息的带宽则会降低.

$b_t$  再由伪随机序列  $p_t$  调制形成调制序列  $b_t \cdot p_t$ , 这里  $p_t \in \{-1, 1\}$  是对普通 0-1 序列的扩充. 调制序列再经  $J(i, j)$  放大, 就形成了待叠加信号序列  $J(i, j) \cdot b_t \cdot p_t$ . 注意, 在对原始图像进行水印信号的叠加时, 我们并不是按照一般的光栅扫描顺序进行的, 而是采用了 Hilbert 扫描顺序, 即  $[i, j] = \text{Hilbert2Matrix}(t, n)$ . Hilbert 扫描具有很强的相关聚类特性, 这使得叠加窗口内的像素值分布较为均匀, 我们会在后面的水印检测算法中作进一步的解释. 经过以上的步骤, 我们就得到了最后的水印图像, 形式如下:

$$I'(i, j) = I(i, j) + J(i, j) \cdot b_t \cdot p_t. \tag{2}$$

由于使用了伪随机序列调制, 加入的水印信号在没有相同的伪随机序列解调的情况下是无法恢复的, 而伪随机序列是根据一个密钥产生的. 用考虑 HVS 特性计算出的噪声阈值矩阵  $J(i, j)$  作

为引入噪声的掩模,保证了在不损害视觉效果的前提下,充分放大了水印信号的能量,也即在不损害水印透明性的同时得到了较好的鲁棒性。

图 4(b)是原始图像 Lena,图 4(a)是利用了 HVS 特性产生的水印图像,图 4(c)是不利用 HVS 特性加入等量幅度相当的水印数据后产生的水印图像。这里,JND 均值为 6,即平均每像素的变换幅度约为 6 个灰度级。很明显,对于图 4(a)肉眼几乎察觉不出什么异样,而图 4(c)则有相当严重的噪声感。



(a) Watermarked image utilizing HVS characteristics

(b) Original Lena

(c) Watermarked image without utilizing HVS characteristics

(a) 利用 HVS 特性的水印图像

(b) 原 Lena 图

(c) 未利用 HVS 特性的水印图像

Fig. 4 Comparison of watermarked images with and without utilizing HVS characteristics

图 4 水印效果比较图

### 1.3 水印检测算法

对应于上述水印嵌入算法,水印检测算法如下。用相同的密钥恢复伪随机序列  $p_t$  对水印图像和伪随机序列  $p_t$  作相关处理,这可以理解为一次解调过程。然后,在以  $cr$  为大小的相关窗口上进行累加。具体计算公式如下<sup>[3,7]</sup>:

$$s_k = \sum_{t=k \cdot cr}^{(k+1) \cdot cr - 1} (p_t \cdot I'(i, j)) = \sum_{t=k \cdot cr}^{(k+1) \cdot cr - 1} (p_t \cdot I(i, j)) + \sum_{t=k \cdot cr}^{(k+1) \cdot cr - 1} (p_t^2 \cdot J(i, j) \cdot b_t). \quad (3)$$

在理想情况下,即

$$\sum_{t=k \cdot cr}^{(k+1) \cdot cr - 1} p_t = 0 \quad (4)$$

及  $I(i, j)$  为常数的条件下,式(3)右边第 1 项等于 0,则

$$s_k = \sum_{t=k \cdot cr}^{(k+1) \cdot cr - 1} (p_t^2 \cdot J(i, j) \cdot b_t) = cr \cdot J(i, j) \cdot b_t. \quad (5)$$

由  $b_t$  与  $w_k$  的关系,得出

$$w_k = \begin{cases} 0 & \text{sign}(s_k) = -1 \\ 1 & \text{sign}(s_k) = +1 \end{cases}, \quad (6)$$

至此恢复出水印信息。

但是,理想条件几乎不可能成立。第 1,图像中的像素值不可能为常数,所以我们利用 Hilbert 扫描增加求和窗口  $[k \cdot cr, (k+1) \cdot cr - 1]$  内的像素相关性来逼近这一要求。第 2,伪随机序列也不能保证在窗口内  $-1$  与  $+1$  的个数正好相等。所以,我们加入修正项:

$$\Delta = - \left( \sum_{t=k \cdot cr}^{(k+1) \cdot cr - 1} p_t \right) \cdot \text{mean}(I'(i, j)). \quad (7)$$

其中  $\text{mean}(I'(i, j))$  计算水印图像在求和窗口  $[k \cdot cr, (k+1) \cdot cr - 1]$  内的均值。

这样,式(3)修改为

$$s_k = \sum_{t=k \cdot cr}^{(k+1) \cdot cr - 1} (p_t \cdot I'(i, j)) + \Delta \approx cr \cdot J(i, j) \cdot b_t, \tag{8}$$

式(6)不变,  $w_k$  就是恢复出的水印信息. 在上述各式中,  $[i, j] = \text{Hilbert2Matrix}(t, n)$ .

当然, 在水印图像经历一些处理、变换或侵权人的恶意攻击后, 提取出的水印可能不会与嵌入的水印完全相同. 这时, 我们需要给出一个判决标准来判定版权水印信息的存在与否. 我们采用提取水印与原始水印的相关性作为衡量标准<sup>[15]</sup>, 公式如下:

$$\text{corr}(w^*, w) = \frac{\sum_{i=1}^N (w_i^* - \overline{w^*})(w_i - \overline{w})}{\sqrt{\sum_{i=1}^N (w_i^* - \overline{w^*})^2} \sqrt{\sum_{i=1}^N (w_i - \overline{w})^2}}. \tag{9}$$

其中  $w^*$  和  $w$  分别是待判决水印和正确的水印,  $\overline{w}$  是向量  $w$  的均值,  $\text{corr}$  取值在  $[-1, 1]$  之间. 如果这一相关值超过某一阈值, 我们就判定图像中存在此水印.

2 实验结果与攻击分析

本文的算法在 PIII50 机器上实现, 编程环境为 MATLAB 5.3.

2.1 阈值确定

为了确定水印检测中相关测试的阈值, 我们进行了阈值确定实验. 方法是随机生成 10 000 个长度为 50 比特的水印信号, 其中第 5 000 个水印信号是原始水印信号. 分别与原始的水印信号作相关检测, 结果如图 5 所示. 实验结果表明, 随机生成的水印信号与正确的水印信号的最大相关值在 0.52 左右. 因此, 我们可以将检测阈值定为 0.55. 为了准确起见, 也可以将其再放大, 以降低系统发生虚检(false positive)的概率. 所谓虚检, 就是将没有水印信号的图像误认为含有水印信号的图像. 但这样将会提高漏检(false negative)概率, 即未能从含有水印信号的图像中检测到水印信号.

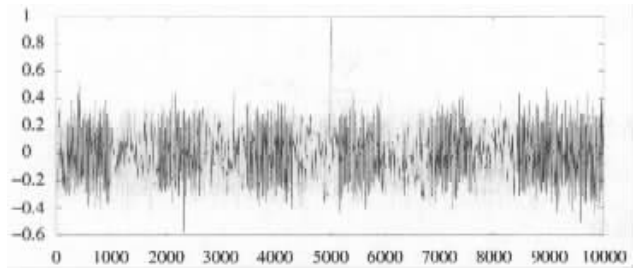


Fig. 5 Watermark detection threshold setting  
图 5 水印判决阈值的确定

2.2 水印嵌入和检测的改进

在实验中我们发现, 如果对水印强度进行一定的自适应调节, 可以在保证水印鲁棒性的同时进一步降低水印信号能量, 即增加水印的透明性. 由水印检测算法, 我们可以将

$$t_k = \text{abs}(s_k) \tag{10}$$

作为衡量水印强度的标准,  $\text{abs}()$  是绝对值函数. 在水印嵌入的同时计算  $s_k$ , 若  $s_k$  超过某一上限, 我们认为水印能量已经足够强, 这时按比例自动降低  $J(i, j)$ , 并修正由式(2)计算得到的水印图像; 若  $s_k$  低于某一下限, 我们认为水印能量太弱, 增加  $J(i, j)$ , 并修正由式(2)计算得到的水印图像. 当



然,下限不能定得过高,否则, $J(i,j)$ 大面积、大幅度地改变,将破坏视觉模型的总体效果,使水印透明性降低.我们根据实验确定的经验值为下限 3 000,上限 6 000.经水印强度自适应调节后的水印图像如图 6(c)所示.



(a) Watermarked image without strength adaptation  
(a) 未经强度调节的水印图像  
(b) Original Lena  
(b) 原 Lena 图  
(c) Watermarked image with strength adaptation  
(c) 水印强度调节后的水印图像

Fig. 6 Comparison of watermarked images with and without strength adaptation

图 6 水印强度自适应调节效果图

为了更加准确地判定水印的存在性,可以在水印检测之前对受过攻击的水印图像进行自动校正,尤其是对受到几何变换攻击的水印图像,这一措施非常有效,校正依据是原始图像.我们考察了著名的水印攻击软件 Stirmark 对我们的水印图像的攻击. Stirmark<sup>[16]</sup>模仿重采样的过程,对水印图像引入轻微的拉伸、剪切、平移、旋转,然后用 Nyquist 插值进行重采样,并同时引入噪声. Stirmark 综合了各种攻击手段,所以攻击力非常强.到目前为止,它可以成功击破所有商业水印系统.在表 1 中我们可以看到,它也成功地攻击了我们的系统,使检测到的相关值下降到 0.28.我们认为对抗此种攻击的有效思路是对受到攻击的图像进行校正.我们实现了一个简单的运动向量检测器,采用 MPEG1 标准中的块匹配法,匹配精度为 1 个像素单位<sup>[17]</sup>.利用运动检测结果对受 Stirmark 攻击的水印图像进行自动校正,然后检测水印,结果相关值上升至 0.89,而另一幅含有不同水印的图像经校正后相关值仍然在阈值以下.实验结果表明,在检测水印之前加入自动校正预处理环节,大大提高了检测水印的准确性,是对付强劲水印攻击的有效手段.

2.3 攻击分析

我们使用 256 \* 256 的 Lena 图作为实验图像,使用上述算法嵌入 50 比特的水印,相应的  $cr = 256 * 256 / 50 \approx 1310$ . 计算得到的 JND 均值为 3.53,即平均每像素的变换幅度约为 3.53 个灰度级.

对水印图像的攻击实验结果总结见表 1. 实验平台采用 JASC 公司的共享软件 PaintShop 5.0. 以下测试结果中的参数如果未加特殊说明,均是在 PaintShop 5.0 平台下相应的参数值.

从攻击实验的结果来看,本文的数字水印算法对一系列信号处理操作具有较强的鲁棒性. 特别是对于叠加噪声、图像增强、二次水印、色彩变换,水印信号的每一位都被正确无误地提取出来了. 另外一个值得注意的问题是,系统对几种线性或非线性滤波的抵抗力也令人满意. 对 JPEG 压缩的抵抗力同样不错,即使在压缩系数等于 90 的低品质条件下,仍然达到了 0.56 的相关值. 对轻微的马赛克效果处理也有抵抗力. Stirmark 攻击在引入被攻击图像自动校正环节以后,同样可以成功地检测到水印信号.

Table 1 Results of the attack experiments  
表 1 攻击实验结果

Processing <sup>①</sup>	Parameters <sup>②</sup>	Correlation <sup>③</sup>
Noise addition <sup>④</sup>	Uniform <sup>⑤</sup> (amount=10)	1.00
	Random <sup>⑥</sup> (amount=10)	1.00
	Histogram equalization <sup>⑧</sup>	1.00
Image enhancement <sup>⑦</sup>	Sharpening <sup>⑨</sup>	1.00
	Strong sharpening <sup>⑩</sup>	1.00
	Edge enhancement <sup>⑪</sup>	1.00
	Strong edge enhancement <sup>⑫</sup>	1.00
Twice watermarking <sup>⑬</sup>	First watermarking <sup>⑭</sup>	1.00
	Second watermarking <sup>⑮</sup>	1.00
Color conversion <sup>⑯</sup>	16-Color dithering <sup>⑰</sup>	1.00
JPEG compression <sup>⑱</sup>	Compression 60	0.89
	Compression 90	0.56
Mosaic <sup>⑲</sup>	Block 2 * 2	0.84
	Block 3 * 3	0.56
Filtering <sup>⑳</sup>	Lowpass filtering <sup>㉑</sup>	0.72
	Median filtering <sup>㉒</sup>	0.72
	Gaussian blur <sup>㉓</sup> (radius=1)	0.72
	Motion blur <sup>㉔</sup> (4 pixels)	0.72
Stretch <sup>㉕</sup>	No rectification <sup>㉖</sup>	0.28
	Rectification using original image <sup>㉗</sup>	0.89
	An image containing a different watermark after rectification <sup>㉘</sup>	0.20

①处理操作,②参数,③相关值,④叠加噪声,⑤均匀分布,⑥随机分布,⑦图像增强,⑧直方图均衡化,⑨锐化,⑩强锐化,⑪边缘锐化,⑫强边缘锐化,⑬二次水印,⑭第一水印,⑮第二水印,⑯色彩变换,⑰16 灰度抖动,⑱JPEG 压缩,⑲马赛克效果,⑳滤波,㉑低通滤波,㉒中值滤波,㉓高斯滤波,㉔运动模糊(4 像素),㉕不校正,㉖使用原始图像校正,㉗一个包含不同水印的图像经校正.

3 结束语

本文提出的水印算法具有以下特点:

- (1) 用考虑 HVS 特性计算出的噪声阈值矩阵  $J(i, j)$  作为叠加水印信号的掩模,保证了水印信号的透明性. 并且,噪声阈值矩阵的计算采用了简化 HVS 模型,直接在空域内计算,复杂度低.
- (2) 水印信号叠加过程采用 Hilbert 扫描顺序进行,改善了求和窗口内的像素相关特性,提高了水印信号提取的准确性.
- (3) 水印强度具有自适应调节能力,在保证水印鲁棒性的同时,进一步增加了水印透明性.
- (4) 水印检测算法可以加入自动校正预处理模块,提高了水印判决的准确性.

由于具有以上特点,本文提出的水印算法具有较好的透明性、鲁棒性,水印检测结果准确,并且算法复杂度较低. 实验结果及对比实验说明了这一点. 进一步增强水印鲁棒性的措施还包括:增大  $cr$ ; 采用校验和纠错码技术编码水印比特流等. 但这些措施都是以降低嵌入水印带宽为代价的. 我们还可以利用混沌序列来代替伪随机序列对水印信号进行调制,由于混沌序列具有优良的特性,有望进一步提高水印鲁棒性<sup>[11]</sup>.

我们今后的工作将主要在以下几个方面进行:

- (1) 研制适用于多种媒体类型和数据格式的鲁棒性好的水印算法和系统:包括文本、图像、声音、视频、三维物体数据的数字水印系统.

(2) 公钥数字水印系统,即作者使用一个专有的密钥来叠加水印信号,而任何人均可通过一个公开的密钥来检测出水印信号,但是,从公开的密钥推导专有密钥和从公开的密钥来去除水印信号这两个过程都是非常困难的.这一目标一旦有所突破,将最大限度地提高水印系统的实用价值,正如公钥系统在传统密码学领域中的贡献一样.

(3) 基于高层信息级别的水印系统.建立于低层符号级的水印系统完全依赖于计算技术,容易受到攻击.而基于更高层的信息特征,比如图像的内容、文本的语意等设计的水印系统,可以具有更好的鲁棒性.

## References:

- [1] Anderson, R. J. Information Hiding: 1st International Workshop. Vol. 1174 of Lecture Notes in Computer Science, Berlin: Springer-Verlag, 1996.
- [2] Bender, W., Gruhl, D., Morimoto, N. Techniques for data hiding. IBM System Journal, 1996, 35(3&4): 313~316.
- [3] Hartung, F., Girod, B. Watermarking of MPEG-2 encoded video without decoding and re-encoding. In: Freeman, M., Jaretzky, P., Vin, H. M., eds. Proceedings of the SPIE Conference on Multimedia Computing and Networking 1997, Vol 3020. Bellingham: SPIE Press, 1997. 264~273.
- [4] Podilchuk, C. I., Zeng, Wen-jun. Digital image watermarking using visual models. In: Rogowitz, B. E., Pappas, T. N., eds. Proceedings of the SPIE Conference on Human Vision and Electronic Imaging II, Vol 3016. Bellingham: SPIE Press, 1997. 100~111.
- [5] Cox, I. J., Kilian, J., Leighton, T., et al. Secure spread spectrum watermarking for multimedia. IEEE Transactions on Image Processing, 1997, 6(12): 1673~1687.
- [6] Fridrich, J., Baldoza, A. C., Simard, R. J. Robust digital watermarking based on key-dependent basis functions. In: Auesmith, D., ed. Information Hiding: 2nd International Workshop. Berlin: Springer-Verlag, 1998. 143~157.
- [7] Kankanhalli, M. S., Rajmohan, Ramakrishnan, K. R. Content based watermarking of images. In: Effelsberg, W., ed. ACM Multimedia 98-Electronic Proceedings, the 6th ACM International Multimedia Conference. New York: ACM Press, 1998.
- [8] Memon, N., Wong, P. W. Protecting digital media content. Communications of the ACM, 1998, 41(7): 35~43.
- [9] Zhao, Jian, Koch, E., Luo, Cheng-hui. In business today and tomorrow. Communications of the ACM, 1998, 41(7): 67~72.
- [10] Yin, Kang-kang, Xiang, Hui, Shi, Jiao-ying. Multimedia watermarking systems and their attack analysis. Computer Science, 1999, 26(10): 44~48 (in Chinese).
- [11] Xiang Hui. Multimedia data compression based on information reordering and multimedia data security [Ph. D. Thesis]. Hangzhou: Zhejiang University, 1999 (in Chinese).
- [12] Griffiths, J. G. Table-Driven algorithms for generating space filling curves. Computer Aided Design, 1985, 17(1): 37~41.
- [13] Takeshi, Agui, Takanori, Nagae, Masayuki, Nakajima. Generalized Peano scans for arbitrarily-sized arrays. IEICE Transactions, 1991, E74(5): 1337~1342.
- [14] Lu, Kai-cheng. Computer Cryptography. Beijing: Qinghua University Press, 1998. 185~196 (in Chinese).
- [15] Press, W. H., Teulkolsky, S. A., Vetterling, W. T., et al. Flannery. Numerical Recipes in C. 2nd ed, London: Cambridge University Press, 1996. 636~639.
- [16] Petitcolas, F. A. P., Anderson, R. J., Kuhn, M. G. Attacks on copyright marking systems. In: Auesmith, D., ed. Information Hiding: 2nd International Workshop. Berlin: Springer-Verlag, 1998. 218~238.
- [17] Yang Pin, Zhong Yu-zhuo, Cai Lian-hong, translated. MPEG coding standards of moving pictures (ISO/IEC 11172). Beijing: Machine Industry Press, 1995. 125~129 (in Chinese).

## 附中文参考文献:

- [10] 尹康康, 向辉, 石教英. 多媒体数据数字水印系统及其攻击分析. 计算机科学, 1999, 26(10): 44~48.
- [11] 向辉. 基于信息重组思想的多媒体数据压缩与多媒体数据安全技术研究[博士学位论文]. 杭州: 浙江大学, 1999.
- [14] 卢开澄. 计算机密码学. 北京: 清华大学出版社, 1998.
- [17] 杨品, 尹平, 郑卓宇, 蔡联红, 译. MPEG 运动图像压缩编码标准(ISO/IEC 11172). 北京: 机械工业出版社, 1995. 125~129.



# A Robust Image Watermarking Algorithm \*

YIN Kang-kang, SHI Jiao-ying, PAN Zhi-geng

(State Key Laboratory of CAD & CG, Zhejiang University, Hangzhou 310027, China)

E-mail: jyshi@cad.zju.edu.cn

http://www.zju.edu.cn

**Abstract:** In this paper, a robust image watermarking algorithm is proposed, which adopts the Hilbert scanning, and uses JND (just noticeable distortion) matrix based on HVS (human visual system) characteristics to mask the watermarking signal when embeds the watermark. And the strength of the watermark can be self-adapting. Auto-Rectification can also be added, which greatly improves the accuracy of watermark detection. Based on the description of the algorithm, experimental results and attack analysis are given. The experimental results show that this algorithm is transparent and robust. The detection results are faithful and the computational cost is low.

**Key words:** steganography; digital watermarking; Hilbert scanning; HVS (human visual system); attack analysis

\* Received September 27, 1999; accepted March 7, 2000

Supported by the National Natural Science Foundation of China under Grant Nos. 60033010, 60083009; the Natural Science Foundation of Zhejiang Province of China under Grant No. RC00048

## 2001 年中国人工智能学会全国学术年会(CAAI-9)

### 征 文 通 知

为了总结我国智能领域所取得的成就,交流最新进展,迎接 21 世纪智能领域的更大挑战,同时祝贺中国人工智能学会智能信息网络专业委员会、教育与科普委员会、可拓工程专业委员会的成立,中国人工智能学会定于 2001 年 10 月 8~10 日在北京召开第 9 次全国学术年会。欢迎高等学校教师、科研院所和企业的科技人员以及博士生硕士生踊跃参加新世纪我国智能领域的第一次学术盛会。

年会期间,将召开中国人工智能学会理事扩大会议,进行理事会换届和增补新理事,请全体理事、各专业委员会以及关心学会发展的广大同仁届时与会。

#### 一、征文范围

本届学术年会的主题是智能与网络。征文领域包括(但不限于):

(1) 基础理论研究:智能的生理学基础、智能的认知学基础、离散数学与逻辑学理论、智能研究的哲学与方法论;

(2) 基本技术研究:知识工程与知识理论,搜索理论与方法,神经网络新模型与新算法,网络智能、分布智能与群体智能,机器学习,人工生命;

(3) 应用技术研究:计算机视觉与模式识别,智能机器人,自然语言理解与机器翻译,海量数据的智能处理,知识发现与数据挖掘,智能控制、智能管理与智能自动化,智能 CAD 与智能 CAI,可拓工程的理论与应用、面向信息网络的智能应用、面向各种应用的专家系统。

#### 二、征文要求

欢迎以电子版(Word 7.0 以上)投稿。来稿请另纸写明论文题目、作者姓名、单位名称、通信地址、电话号码、E-mail 地址、论文所属领域。论文纸型为 A4,单面,不分栏,5 号字,激光打印,篇幅限为 4 页,最多不超过 6 页。

#### 三、重要日期

征文截止日期:2001 年 8 月 10 日

#### 四、联系方式

(1) 投寄方式: E-mail: yxzhong@ieee.org(电子投稿);100876 北京邮电大学 钟义信教授(邮寄稿件)

(2) 联系电话:010-62282638 或 62283163

(3) 会议网址: <http://www.bupt.edu.cn/~icii/link/index.htm> (学术会议/CAAI-9)