一种强壮的图象水印算法*

尹康康[1]　　石教英[1]　　潘志庚[1, 2]

[1](浙江大学CAD&CG国家重点实验室 杭州 310027)

[2](香港理工大学电子计算学系 香港 九龙)

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

摘要　提出了一种强壮的数字图象水印算法。算法采用 Hilbert 扫描顺序，用考虑 HVS 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。实验表明该算法具有较好的透明性和强壮性，水印检测结果准确，并且算法复杂度较低。

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

1. 简介

多媒体数据的数字化为多媒体信息的存取、处理和传播提供了极大的便利，也极大地提高了信息表达的效率和准确性。但是一个明显的副作用是：多媒体数据的非法传播和拷贝非常容易，而且质量不受损害。在当今这个信息时代，对于多媒体作品的创作者、发行人和版权持有人来说，知识产权保护已成为一项最为紧迫的任务。起源于信息隐藏技术的数字水印技术，为实现有效的知识产权保护提供了一条崭新的思路，近年来已成为多媒体信息安全研究领域的一个热点问题。

1．1 信息隐藏

1996 年 5 月 30 日-6 月 1 日，在英国剑桥牛顿研究所召开了第一界国际信息隐藏学术研讨会，标志着

*本项研究工作由国家自然科学基金提供资助(No. 69773020, 69823003). 尹康康，硕士研究生，主要研究方向为多媒体、计算机图形学. 石教英，教授，博士生导师，主要研究方向为多媒体、虚拟现实和科学计算可视化等. 潘志庚，研究员，博士生导师，主要研究方向为多媒体、分布式图形和虚拟现实技术.

一门新兴的交叉学科——信息隐藏学的诞生。

信息隐藏（Steganography 或 Information Hiding）主要研究如何将一个讯息隐藏起来，致使可能的监察者甚至不知道有这样一个讯息在发送，而密码学中的监察者是知道有一个秘密讯息在发送的，这是信息隐藏与传统密码学的一个本质不同。这就象一个人可以用奇怪的文字书写他要发送的讯息，也可以用看不见的墨水写他要发送的讯息。

图 1 是在第一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相关术语[1]。其中数据类型可以是“ 文本”、“ 消息”、“ 图象”、“ 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。

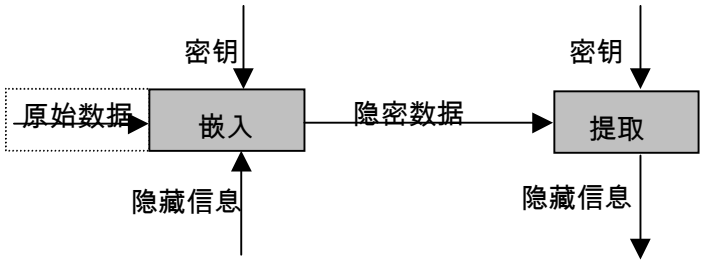

图 1：信息隐藏核心系统参考模型

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、通讯、保密学及信号处理等领域有着广阔的应用背景。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。

1．2 数字水印

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。水印与源数据（如图象、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。

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:(a)透明性(隐藏性);(b) 强壮性(鲁棒性);(c) 隐藏位置的安全性。

近年来,多媒体技术与 Internet 技术发展迅速,使得多媒体数据的安全问题,也就是版权保护问题,成了一项重要而紧迫的研究课题。采用传统密码学理论开发出来的加解密系统,包括经典的密钥系统如 DES(data encryption standard)和安全性更好的公钥系统如 RSA 系统,对于待加密文件的处理是将其加密成密文,使得在网络传递过程中的非法拦截者无法从中获取机密信息,达到保密的目的。但是传统的加密系统并不能很好地解决版权保护问题。因为虽然经过加密后,只有被授权持有解密密钥的人,才可以存取数据,但是这样就无法向更多的人展示自己的作品;而且数据一旦被解开,就完全置于解密人的控制之下,原创作者没有办法追踪作品的复制和转发。网络多媒体时代需要一种更加有效的技术手段来保护多媒体信息的著作权。数字水印技术为实现有效的信息版权保护手段提供了一条崭新的思路,成为多媒体信息安全研究领域的一个热点问题,逐渐得到重视。

1.3 相关工作

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[2, 3, 4, 5, 6, 7]。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[8,9]。有关具体内容请参考[10]。

本文提出的数字水印算法属于空域水印算法,并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[3]和 Kankanhalli 算法[7]。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,求和窗口内象素相关性差;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象,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 和 Kankanhalli 算法中存在的这些缺陷。

本文第二节是水印算法描述，第三节给出相关实验及攻击分析，最后给出算法总结和讨论。

2．强壮图象水印算法

2．1 Hilbert 扫描

Hilbert扫描是一种空间填充曲线[11]。通常在将二维图象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象中一个方向的相关性。Hilbert扫描可以很好地保留二维相关性。图 2 中给出了 3 阶Hilbert曲线的示意图，由图示可以看出，这种扫描的盘旋结构将图象中具有高相关性的数据汇集到了一起。对于 $2^n \times 2^n$的图象，我们可以递归地构造n阶的Hilbert曲线[12]。我们给出两个抽象的递归函数*[i,j]=Hilbert2Matrix(t,n)*和*[t]=Matrix2Hilbert(i,j,n)* ,进行一维Hilbert曲线中某个象素点的下标*t*与其在图象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[13]，使得其应用更加具有灵活性。

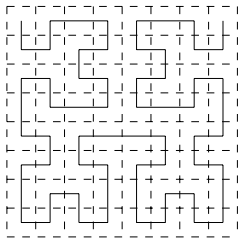

图 2. 3 阶 Hilbert 曲线

2．2 水印嵌入算法

算法基本框图如图 3 所示。为了算法描述上的简单，采用 256 级的灰度图象作为原始图象。算法的基本思想是将水印信号的比特流转化成类似噪声的信号加入图象中，即对每个象素点的灰度值做轻微扰动，使其携带水印信息。考虑到透明性和强壮性的要求，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 HVS (Human Visual System) 特性的噪声分配，位扩展，用伪随机序列[14]调制水印信息，采用 Hilbert 扫描。

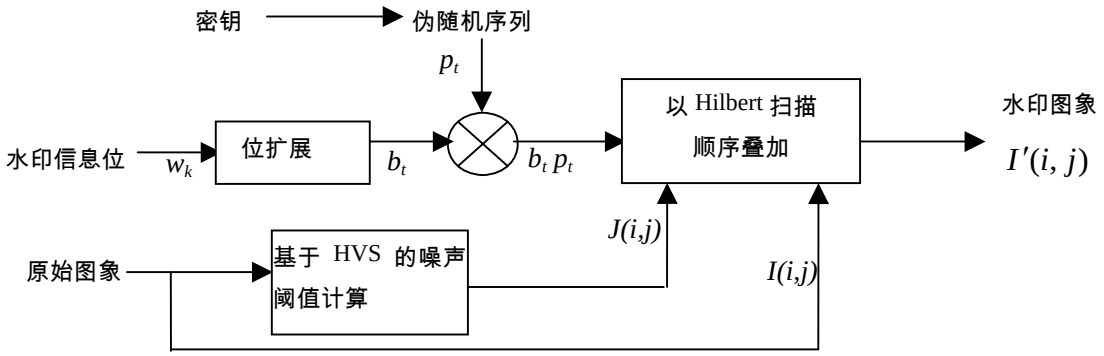

图 3. 水印算法示意图

图 3 中 $I(i,j)\{1\le i\le n, 1\le j\le n\}$代表原始图象中第 i 行第 j 列象素的灰度值。$J(i,j)$是考虑人眼视觉特性计算出的(i,j)点的可感知噪声阈值(JND: just noticeable distortion，或称恰可察觉失真)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知。

我们的阈值计算主要利用了 HVS 的三个特性[7]：人眼对不同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；对图象平滑区的噪声敏感，对纹理区的噪声不敏感；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。

具体计算 $J(i,j)$如下。首先将图象分成 8×8 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象块分成 8 类，为每一类指定一个基准的噪声阈值。然后对每个象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，这个值加上该象素所在小图象块的基准噪声阈值，就形成了象素 $I(i,j)$ 的可感知噪声阈值 $J(i,j)$。图象块的分类数量、图象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象确定，但也可为了简化起见，对不同复杂度的图象给出一组代表值。细节丰富的图象复杂度高，平滑的图象复杂度低。

需要指出，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，会影响数字水印系统的处理效率。

下面说明水印算法流程。

$$b_t = \begin{cases} 1, & w_k = 1 \\ -1, & w_k = 0 \end{cases} \qquad k \cdot cr \le t < (k+1) \cdot cr \qquad (1)$$

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

位扩展[3]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$J(i,j) \cdot b_t \cdot p_t$。注意在对原始图象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]=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象素值分布较为均匀，后面我们会在水印检测算法中作进一步的解释。

$$I'(i,j) = I(i,j) + J(i,j) \cdot b_t \cdot p_t \qquad (2)$$

经过以上的步骤，我们就得到了最后的水印图象，形式如下：

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强壮性。

图 4b 是原始图象 Lena，图 4a 是利用了 HVS 特性产生的水印图象，图 4c 是不利用 HVS 特性加入等量幅度相当的水印数据产生的水印图象。这里 JND 均值为 6,即平均每象素的变换幅度约为 6 个灰度级。很明显，左图肉眼几乎察觉不出什么异样，而右图有相当严重的噪声感。

(a) 利用 HVS 特性的水印图象　　(b) 原 Lena 图　　(c) 未利用 HVS 特性的水印图象

图 4. 水印效果比较图

2．3 水印检测算法

对应上述水印嵌入算法，水印检测算法如下。用相同的密钥恢复伪随机序列p_t,对水印图象和伪随机序列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[3,7]：

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

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

在理想情况下，即

及 $I(i,j)$为常数的条件下，(3)式右边第一项等于零。那么

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

由b_t与w_k的关系,得出

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

至此恢复出水印信息。

但是，理想条件几乎不可能成立。第一，图象中的象素值不可能为常数，所以我们利用 Hilbert 扫描增加求和窗口$[k \cdot cr, (k+1) \cdot cr - 1]$内的象素相关性来逼近这一要求。第二，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

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

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

这样(3)式修改为

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

（6）式不变，w_k就是恢复出的水印信息。上述各式中*[i,j]=Hilbert2Matrix(t,n)*。

当然，在水印图象经历一些处理、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[15]。公式如下：

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

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，*corr* 取值在[-1,1]之间。如果这一相关值超过某一阈值，我们就判定图象中存在此水印。

3．实验结果与攻击分析

本文算法在 PII 350 机器上实现，编程环境为 MATLAB 5.3。

3．1 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 10000 个长度为 50 比特的水印信号，其中第 5000 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。结果见图 5。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的概率。所谓虚检(false positive)，就是将没有水印信号的图象误认为含有水印信号。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象中检测到水印信号。

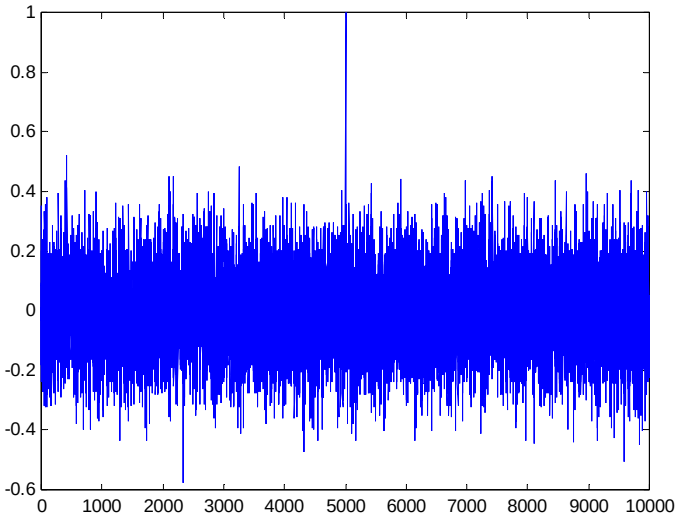

图 5.水印判决阈值的确定

3．2 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，可以在保证水印强壮性的同时进一步降

$$t_k = abs(s_k) \qquad (10)$$

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

作为衡量水印强度的标准, *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（2）式计算得到的水印图象；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（2）式计算得到的水印图象。当然，下限不能定得过高，否则$J(i,j)$大面积大幅度改变，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 3000，上限 6000。经水印强度自适应调节后的水印图象如图 6 中的(c)图。

(a)未经强度调节的水印图象　　(b) 原 Lena 图　　(c)水印强度调节后的水印图象

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象进行自动校正，尤其对受到几何变换攻击的水印图象，这一措施非常有效，校正依据是原始图象。我们考察了著名的水印攻击软件 Stirmark 对我们水印图象的攻击。Stirmark [16]模仿重采样的过程，对水印图象引入轻微的拉伸、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，到目前为止可以成功击破所有商业水印系统。在表 1 中我们将看到，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象进行校正。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 个象素单位[17]。利用运动检测结果对受 Stirmark 攻击的水印图象进行自动校正，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象经校正后相关值仍然在阈值以下。实验结果证明，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。

3．3 攻击分析

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

对水印图象的攻击实验结果总结于表 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 中相应的参数值。

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、图象增强、二次水印、色彩变换，水印信号每一位都正确无误地提取出来了。另外一个值得注意的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象自动校正环节后，同样可以成功检测到水印信号。

处理操作	参数	相关值
叠加噪声	均匀分布 （amount=10）	1.00
	随机分布 （amount=10）	1.00
图象增强	直方图均衡化	1.00
	锐化	1.00
	强锐化	1.00
	边缘锐化	1.00
	强边缘锐化	1.00
二次水印	第一水印	1.00
	第二水印	1.00
色彩变换	16 灰度抖动	1.00
JPEG 压缩	Compression 60	0.89
	Compression 90	0.56
马赛克效果	Block 2*2	0.84
	Block 3*3	0.56
滤波	低通滤波	0.72
	中值滤波	0.72
	高斯滤波(radius=1)	0.72
	运动模糊（4 象素）	0.72
Stirmark	不校正	0.28
	使用原始图象校正	0.89
	一含不同水印的图象经校正	0.20

表 1.攻击实验结果

4．结语

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象素相关特性，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，在保证水印强壮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、强壮性，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。进一步增强水印强壮性的措施还包括：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强壮性[11]。

我们今后的工作将主要在以下几方面进行：

1．研制适用于多种媒体类型和数据格式的强壮水印算法和系统：包括文本、图象、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。而基于更高层信息特征，比如说图象的内容，文本的语意等设计的水印系统，可以具有更高的强壮性。

参考文献

1 Anderson R J ed. Information Hiding: First 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 Systems 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, Jardetzky P, Vin H M eds. Proceedings of SPIE Conference on Multimedia Computing and Networking 1997, volume 3020. Bellingham: SPIE Press, 1997. 264~273

4 Podilchuk C I, Zeng W. Digital Image Watermarking using Visual Models. In: Rogowitz B E, Pappas T N eds. Proceedings of SPIE Conference on Human Vision and Electronic Imaging Ⅱ, 1997, volume 3016. Bellingham: SPIE Press, 1997. 100~111

5 Cox I J, Kilian J, Leighton T, Shamoon T. 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: Aucsmith D ed. Information Hiding: Second International Workshop. Berlin: Springer Verlag, 1998. 143~157

7 Kankanhalli M S, Rajmohan, Ramakrishnan K R. Content Based Watermarking of Images. http://www.acm.org/sigs/sigmm/MM98/electronic_proceedings/kankanhalli/index.html. In: Effelsberg W ed. ACM MULTIMEDIA 98-Electronic Proceedings http://www.acm.org/sigs/sigmm/MM98/electronic_proceedings. Bristol, UK, The Sixth 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 J, Koch E, Luo C. 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

(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 Xiang Hui. Multimedia Data Compression Based on Information Reordering and Multimedia Data Security. Ph.D. Thesis, Zhejiang University, 1999

(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，浙江大学, 1999)

12 Griffiths J G. Table-driven Algorithms for Generating Space Filling Curves. Computer Aided Design, 1985, 17(1): 37~41

13 Agui T, Nagae T, Masayuki, Nakajima. Generalized Peano scans for arbitrarily-sized arrays. IEICE(Institute of Electronics, Information and Communication Engineers) Transactions, 1991, E74(5): 1337~1342

14 Lu Kai-cheng. Computer Cryptography. Beijing: Qinghua University Press, 1998. 185~196

(卢开澄．计算机密码学．北京：清华大学出版社, 1998. 185~196)

15 Press W H, Teulkolsky S A, Vetterling W T, Flannery B P. 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: Aucsmith D ed. Information Hiding: Second International Workshop. Berlin: Springer Verlag, 1998. 218~238

17 Translator: Yang Pin, Zhong Yu-zhuo, Cai Lian-hong. MPEG coding standards of moving pictures (ISO/IEC 11172). Beijing: Engineering Industry Press, 1995. 125~129

(杨品，钟玉琢，蔡莲红 译. MPEG 运动图象压缩编码标准(ISO/IEC 11172)．北京：机械工业出版社, 1995. 125~129)

A Robust Image Watermarking Algorithm

YIN Kang-kang[1] SHI Jiao-ying[1] PAN Zhi-geng[1, 2]

[1](*State Key Lab of CAD&CG Zhejiang University Hangzhou* 310027)

[2] (*Dept. of Computing Hong Kong Polytechnic University Hung Hom Kowloon Hongkong*)

Abstract A robust image watermarking algorithm is proposed. This algorithm adopts the Hilbert scanning, uses JND matrix based on HVS 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 experiments show that it is transparent and robust. The detection results are faithful. The computational cost is low.

Key words Steganography, Digital Watermarking, Hilbert scanning, HVS, Attack analysis

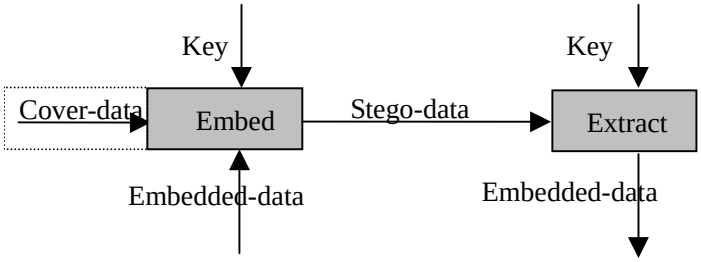

Figure 1. Reference model of core components in stegosystem

Figure 2. The third order Hilbert curve

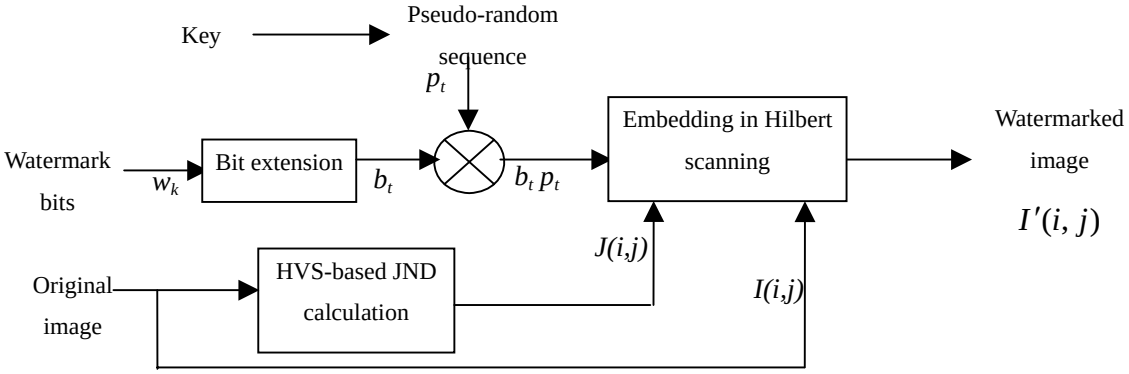

Figure 3. Watermarking algorithm illustration

(a) Watermarked image utilizing HVS characteristics (b) Original Lena (c) watermarked image without utilizing HVS characteristics

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

Figure 5. Watermark detection threshold setting

(a)Watermarked image without strength adaptation (b) Original Lena (c)Watermarked image with strength adaptation

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

PROCESSING	PARAMETERS	CORRELATION
Noise addition	Uniform （amount=10）	1.00
	Random （amount=10）	1.00
Image enhancement	Histogram equalization	1.00
	Sharpening	1.00
	Strong sharpening	1.00
	Edge enhancement	1.00
	Strong edge enhancement	1.00
Second watermarking	First watermarking	1.00
	Second watermarking	1.00
Color conversion	16-color dithering	1.00
JPEG compression	Compression 60	0.89
	Compression 90	0.56
Mosaic	Block 2*2	0.84
	Block 3*3	0.56
Filtering	Lowpass filtering	0.72
	Median filtering	0.72
	Gaussian Blur (radius=1)	0.72
	Motion Blur（4 pixels）	0.72
Stirmark	No rectification	0.28
	Rectification using original image	0.89
	An image containing a different watermark after rectification	0.20

Table 1. Results of the attack experiments