基于 Hilbert 填充曲线的自适应隐写

戴跃伟,刘光杰,叶曙光
(南京理工大学自动化学院,江苏南京 210094)

摘 要: 自适应隐写用于将适量的消息比特嵌入到载体以取得感知质量和容量的最佳折衷.本文提出一种基于量化嵌入机制的自适应隐写方法,并基于该方法将秘密消息比特嵌入到由 Hilbert 填充曲线顺序构造的三像素组的两像素差中.由于充分利用图像本身的感知特性构造了量化嵌入使用的分割码本,所提算法在感知质量和容量上具有较好的综合性能.

关键词: 隐写; 基于量化的嵌入; Hilbert 填充曲线
中图分类号: TP309.7 **文献标识码**: A **文章编号**: 0372-2112 (2008) 12A-035-05

Adaptive Steganography Based on Hilbert Filling Curve

DAI Yue-wei, LIU Guang-jie, YE Shu-guang
(*School of Automation, Nanjing University of Science and Technology, Nanjing, Jiangsu* 210094, *China*)

Abstract: Adaptive steganography is to embed moderate message bits to gain the optimum trade-off between capacity and imperceptibility. In this paper, an adaptive steganographic method is proposed based on the quantization-based embedding mechanism. The message bits are embedded into triple-pixel differences constructed by the Hilbert curve scanning order through the proposed method. Because the partition codebook used in the quantization-based embedding phase is built up based on the perceptual characteristics, the proposed method can achieve good performance both on capacity and distortion.

Key words: steganography; quantization-based emebdding; hilbert filling curve

1 引言

容量、感知质量和安全性是隐写算法设计中最为重要的三个要素.如何在隐藏数据的过程中取得感知质量和容量之间的折衷一直是研究者感兴趣的课题. Wu[1]提出在图像值差中隐藏信息的方法,该方法首先将图像分成由相邻两个像素组成的小块,然后通过修改小块中两个像素的差值来实现消息比特的嵌入.在文献[2]中, Ming 等人通过引入模函数改进了 Wu 的方法,可实现更大的嵌入容量.基于图像像素间关系的更一般的边界匹配的隐写方法是由 Chang 和 Tseng 在文献[3]中提出的.在文献[4]中,我们提出了一种基于神经网络预测误差的隐写算法,该方法通过类似于 Wu 的手段将数据嵌入到图像的预测误差中.文献[5]中, Park 等人提出了利用两个相邻像素相对于目标像素的差值来决定嵌入数据量,他们还在文献[6]中提出一种类似的利用目标像素邻域内的最大最小值的差来决定嵌入的数据量的方法.张新鹏等人[7]提出一种根据目标图像周围像素组的方差来进行多基符号转换以实现数据嵌入的方法. Yang 和 Lin[8]提出一种面向基的隐藏方法,这种方法将每个块根据基的值来确定类型,并根据预先确定的一系列参数来完成在不同类型块中的数据嵌入. Yang 的方法必须进行大量的检查计算以保证重产生的基与原始的基一致,但其所取得的性能较其他已有方法均优.

本文从量化嵌入的角度,提出一种新的自适应嵌入机制,并将这一机制实施在 Hilbert 扫描的三像素组的两个差分值上.比较已有的自适应方案,本文所提供的自适应机制具有更好的普适性且方便在其他的域中推广实现.

2 量化嵌入机制

2.1 问题的定义

设载体信号 X 由元素 $x_1, x_2, \cdots, x_l$ 组成, x_i 属于包含 M 个元素的值域空间 S,其可分割成 n 个子空间 $\Sigma = (S_1, S_2, \cdots, S_n)$,并且满足:

$$S = \bigcup_{i=1}^{n} S_i, [S_i \cap S_j]_{i \neq j} = \Phi, |S_i| = \Delta_i \qquad (1)$$

这里,$|\cdot|$ 表示集的势,因此每个子空间 S_i 包含 Δ_i 个元素 $(s_{i,1}, s_{i,2}, \cdots, s_{i,\Delta_i})$ 利用不同的指标 $(1, 2, \cdots, \Delta_i)$ 可将

收稿日期:2008-10-23;修回日期:2008-12-18
基金项目:江苏省自然科学基金(No.BK2008403);中国博士后基金(No.20070421017)

消息比特调制到载体信号上.我们称 Σ 为分割码本.

对于载体信号 x,设嵌入的消息比特串为 b,则数据嵌入可表示成如下方程:

$$\begin{aligned} S_k &= \Phi(x) \\ y &= \Psi(S_k, \vartheta(b, \Delta_k)) \end{aligned} \tag{2}$$

这里,量化函数 $\Phi: S \rightarrow \Sigma$ 表示将载体信号 x 映射到子空间 S_k,转换函数 ϑ 将消息比特串转换成整数指标 j,函数 Ψ 将指标 j 映射到对应的元素 s_{kj} 上实现消息比特的嵌入.相应地,解码的过程可利用如下的方程表示:

$$\begin{aligned} S_k &= \Theta(y) \\ b &= \vartheta^{-1}(\Psi^{-1}(y, S_k), |S_k|) \end{aligned} \tag{3}$$

方程(3)中的函数 Θ 用来寻找隐写信号 y 所属的子空间 S_k,Ψ^{-1} 用于提取出 y 在 S_k 中对应的指标,ϑ^{-1} 用来将指标转换成相应的消息比特串.因此,我们可以将基于量化的嵌入写成关于 $(\Sigma, \Phi, \vartheta, \Psi)$ 的四元组.若量化函数 Φ 将 x 映射到其所在的子空间 S_i,即 $\Theta = \Phi$,那么我们称这种量化函数为封闭的.本文考虑一种如式(4)的特殊的量化嵌入形式,其中 Φ 为封闭的量化,ϑ 为二进制到 Δ_i 进制的转化,Ψ 为按照索引来获得对应的子空间的元素,称这种形式的量化嵌入为简单量化嵌入.

$$\begin{aligned} &\Phi(x) = \{s \mid s \in S_i, x \in S_i\} \\ &\vartheta(b, \Delta_i) = j \\ &\Psi(S_i, \vartheta(b, \Delta_i)) = S_{i, \vartheta(b, \Delta_i)} \end{aligned} \tag{4}$$

2.2 容量和失真分析

设消息比特服从 $\{0,1\}$ 上的均匀分布,且载体信号满足统计分布 $P_c = [p_c(s_1), p_c(s_2), \cdots, p_c(s_M)]$,用每个载体信号上能承载的平均比特数来刻画隐写的容量.不难得到能够嵌入到每个样本上的平均比特数目.

$$C(\Sigma, \Phi, \vartheta, P_c) = \sum_{i=1}^{M} p_c(s_i) \cdot \log_2 |\Phi(s_i)| \tag{5}$$

设载体信号为 $X = [x_1, x_2, \cdots, x_L]$,隐写信号为 $Y = [y_1, y_2, \cdots, y_L]$,采用加权平均距离的方式来表示失真,可定义成如下的失真度.

$$D(X, Y) = \frac{1}{L} \sum_{i=1}^{L} w_i \cdot d(x_i, y_i) \tag{6}$$

二元函数 $d(\cdot, \cdot)$ 是某种距离函数(如 Euclid 距离),w_i 可定义为依赖于载体信号 x_i 或其所在的图像局部区域的权因子.若权因子仅依赖于 x_i,则可依据数据嵌入引起的从 s_i 到 s_j 的转移概率 $T(s_i, s_j)$,将失真重新写作:

$$D(X, Y) = \sum_{i=1}^{M} w(s_i) \cdot p_c(s_i) \cdot \sum_{j=1}^{M} T(s_i, s_j) \cdot d(s_i, s_j) \tag{7}$$

简单量化嵌入的转移概率矩阵具有如下的形式:

$$T = \begin{bmatrix} A_{\Delta_1 \times \Delta_1} & 0 & \cdots & 0 \\ 0 & A_{\Delta_2 \times \Delta_2} & \cdots & 0 \\ \cdots & \cdots & \ddots & 0 \\ 0 & 0 & 0 & A_{\Delta_k \times \Delta_k} \end{bmatrix}_{M \times M} \tag{8}$$

以上分析揭示了:如要在载体中嵌入更多的比特数据,要使得载体信号所属子空间的势 Δ 足够大,然而较大的 Δ 同时带来较大的失真.因此隐写算法的性能完全由分割码本 Σ 决定,而设计隐写算法的关键也在于设计合适的分割码本 Σ.

3 自适应隐写方法

Hilbert 空间填充曲线是由德国的数学家 David Hilbert 在 1891 年首次提出的连续分形空间填充曲线.同其他填充曲线相比,Hilbert 曲线具有更好的局部保持特性.利用 Hilbert 曲线构造图像像素空间连续的扫描方式,相比其他如光栅扫描或者 zig-zag 扫描的形式而言,Hilbert 曲线具有更好的空间连续性,这种好的空间连续性能更准确的描述图像的局部像素的空间相关性[9],较好的局部相关特性可以更好地反映图像局部的掩蔽效应,使得嵌入引起的失真控制在较低的水平.图 1 给出了 32 ×32 大小的矩阵的 Hilbert 空间填充曲线的例子.

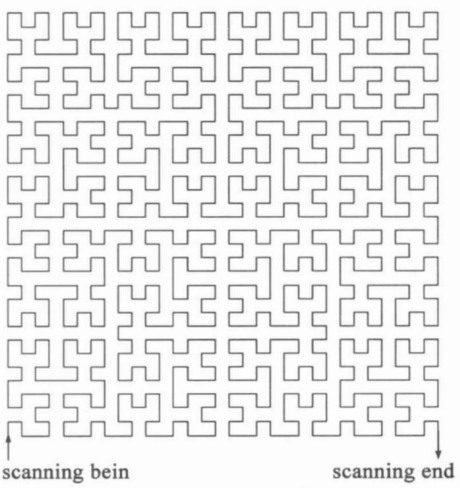


图1 32×32尺寸图像的Hilbert空间填充曲线

利用填充曲线扫描图像可得到一维的像素序列,取连续 3 个像素的两个像素差作为数据嵌入的载体.假设载体图像由 $M \times N$ 个像素组成,因此就有 $L = \lfloor M \times N/3 \rfloor$ 三像素组能用来承载消息比特,L 个二元差分值为 $[(x_{1,1}, x_{1,2}), (x_{2,1}, x_{2,2}), \cdots, (x_{L,1}, x_{L,2})]$,$(x_{i,1}, x_{i,2})$ 通过 $x_{i,1} = p_{i,2} - p_{i,2}$,$x_{i,2} = p_{i,2} - p_{i,3}$,计算得到,其中 $p_{i,1}$,$p_{i,2}$ 和 $p_{i,3}$ 组成一个三像素组.数据的嵌入和提取过程如下.

3.1 数据的嵌入

差分值值域空间为 $S = \{-255, -254, \cdots, -1, 0, 1,$

…,255},设预先设计的分割码本为 Σ,并以密钥 k_1 控制像素组的选择顺序. 对当前的三像素组 $p_{i,1}$, $p_{i,2}$和 $p_{i,3}$,计算$(x_{i,1}, x_{i,2})$,然后根据如式(9)的嵌入算法进行嵌入.

$$\begin{aligned} x'_{i,1} &= \Psi(\Phi(x_{i,1}), \vartheta(b, |\Phi(x_{i,1})|)) \\ x'_{i,2} &= \Psi(\Phi(x_{i,2}), \vartheta(b, |\Phi(x_{i,2})|)) \end{aligned} \tag{9}$$

在消息嵌入到$(x_{i,1}, x_{i,2})$之后,相应地要修改三像素组 $p_{i,1}$, $p_{i,2}$和 $p_{i,3}$的值. 假设 $p_{i,1}$, $p_{i,2}$和 $p_{i,3}$的改变量分别是$\Delta p_{i,1}$,$\Delta p_{i,2}$和$\Delta p_{i,3}$,可通过求解如(10)的优化问题得到$\Delta p_{i,1}$,$\Delta p_{i,2}$和$\Delta p_{i,3}$的值.

$$\begin{aligned} &\min \Delta p_{i,1}^2 + \Delta p_{i,2}^2 + \Delta p_{i,3}^2 \\ &\text{st. } \Delta p_{i,1} - \Delta p_{i,2} = x'_{i,1} - x_{i,1} = \Delta x_{i,1} \\ &\quad \Delta p_{i,2} - \Delta p_{i,3} = x'_{i,2} - x_{i,2} = \Delta x_{i,2} \\ &\quad 0 \le p_{i,1} + \Delta p_{i,1} \le 255 \\ &\quad 0 \le p_{i,2} + \Delta p_{i,2} \le 255 \\ &\quad 0 \le p_{i,3} + \Delta p_{i,3} \le 255 \end{aligned} \tag{10}$$

将$\Delta p_{i,1}$作为问题(10)的变量,我们可得到如式(11)的可行解域.

$$\begin{aligned} &\Delta p_{i,1} \in \Omega = \Omega_1 \cap \Omega_2 \cap \Omega_3 \\ &\Omega_1 = [-p_{i,1}, 255 - p_{i,1}] \\ &\Omega_2 = [-p_{i,2} + \Delta x_{x,1}, 255 - p_{i,2} + \Delta x_{x,1}] \\ &\Omega_3 = [-p_{i,2} + \Delta x_{x,1} + \Delta_{x,2}, 255 - p_{i,2} + \Delta x_{x,1} + \Delta x_{x,2}] \end{aligned} \tag{11}$$

若 $\Omega \neq \varnothing$,则 $\Delta p_{i,1}$, $\Delta p_{i,2}$和 $\Delta p_{i,3}$为:

$$\Delta p_{i,1} = \begin{cases} \left\lfloor \frac{2\Delta x_{i,1} + \Delta x_{i,2}}{3} \right\rfloor & \left\lfloor \frac{2\Delta x_{i,1} + \Delta x_{i,2}}{3} \right\rfloor \in \Omega \\ LB(\Omega) & \left\lfloor \frac{2\Delta x_{i,1} + \Delta x_{i,2}}{3} \right\rfloor < LB(\Omega) \\ RB(\Omega) & \left\lfloor \frac{2\Delta x_{i,1} + \Delta x_{i,2}}{3} \right\rfloor > RB(\Omega) \end{cases} \tag{12}$$

$$\begin{aligned} \Delta p_{i,2} &= \Delta p_{i,1} - \Delta x_{i,1} \\ \Delta p_{i,3} &= \Delta p_{i,1} - (\Delta x_{i,2} + \Delta x_{i,1}) \end{aligned}$$

这里 $LB(\Omega)$和 $RB(\Omega)$分别指 Ω的左边界和右边界.

为避免在 $\Omega = \varnothing$的情况下嵌入数据,对每个三像素组在数据嵌入前做相应的可嵌入性检查. 检查通过计算如下的最大左边界和最小右边界实现.

$$\begin{aligned} &D_1 = |\Phi(p_{i,1} - p_{i,2})| - 1; \\ &D_2 = |\Phi(p_{i,2} - p_{i,3})| - 1; \\ &L = \max(-p_{i,1}, p_{i,2} + D_1, -p_{i,3} + D_1 + D_2) \\ &R = \min(255 - p_{i,1}, 255 - p_{i,2}, + D_1, 255 - p_{i,2} + D_1 + D_2) \end{aligned} \tag{13}$$

假如最大左边界小于最小右边界,即 $L < R$,当前的像素组可实施嵌入,反之放弃嵌入迭代到下一像素组.

3.2 数据的提取

为了正确地提取消息比特,接受端首先必须得到分割码本 Σ,并且利用密钥 k_1 选择像素组 i,并根据式(13)进行可嵌入检查. 当 $L < R$,接收端利用式(14)提取 b_1 和 b_2. 当 $L \ge R$ 时,说明没有进行嵌入,不进行提取. 可嵌入性检查虽然会损失一定承载容量,却可以避免记录嵌入的位置而引起的边信息问题.

$$\begin{aligned} d_1 &= p_{i,1} - p_{i,2} \\ d_1 &= p_{i,2} - p_{i,3} \\ b_1 &= \vartheta^{-1}(\Psi^{-1}(d, \Phi(d_1)), |\Phi(d_1)|) \\ b_2 &= \vartheta^{-1}(\Psi^{-1}(d, \Phi(d_2)), |\Phi(d_2)|) \end{aligned} \tag{14}$$

将所有提取的消息比特连接在一起即可得到最终的解码信息.

3.3 分割码本的构造

对于较大的差分值,像素组所在的区域具有较强的边缘或具有较复杂的纹理,对这类像素组可做较大程度的改动,因此对应的分割码本的子空间尺寸较大. 相反地,较小差分值意味着图像的平滑区域,此类区域不适合进行较大的改动,反映在码本设计上就是相应的子空间的尺寸也较小. 基于以上观察,利用如下的幂次方程构造分割码本.

$$\begin{aligned} &\Delta_n = [a + bn^{\alpha}], n \in [1, K] \\ &\text{s.t.} \quad \alpha \ge 0 \\ &\quad \sum_{n=1}^{K} \Delta_n = 255 \\ &\quad \bmod(K, 2) = 1 \end{aligned} \tag{15}$$

图 2 给出了在参数取 $a = -0.1$, $b = 1.8$, $\alpha = 1.3$ 和 $K = 11$ 情况下分割码本的图例,这一组参数一定程度满足了 HVS 的特性,当然也可采用其他参数来构造分割码书,以实现对不同容量或者感知质量的要求.

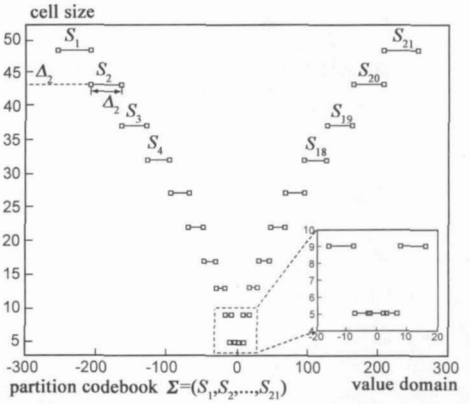


图2 a=-0.1,b=1.8,α=1.3和K=11时的分割码本

综上,图 3 描述了整个自适应隐写的过程. 载体图像首先输入到 Hilbert 曲线扫描中产生空间连续的扫描顺序. 通过子密钥 k_1 控制像素组的选择,并将其输入到可嵌入检查中,若检查通过实施 QBE、像素值修改等操作,若不通过继续进行选择. 该方案中可固定分割码本

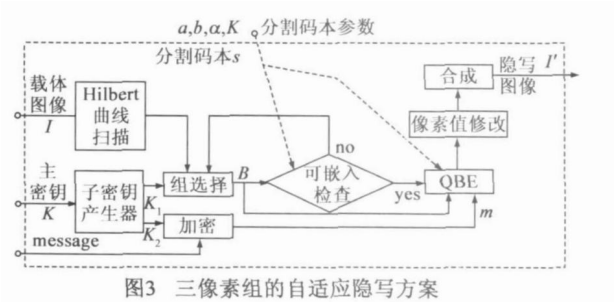


图3 三像素组的自适应隐写方案

的参数以保证使用者的提取,亦可作为额外密钥传送给接收端. 也可采用部分像素以 LSB 方式将参数嵌入到载体,或在隐写图像上实施可逆信息隐藏技术嵌入参数,以供接收端提取.

4 实验结果

选择具有不同平滑程度的四幅 512 ×512 标准测试图像,它们分别为"Lena","Baboon","Peppers"和"Jet". 表 1 给出了容量和失真指标. 在失真程度评价上,分别采用了 *PSNR*, *wPSNR* 和 *mssim* 三种指标,其中 *wPSNR*[10]和 *mssim*[11]都是被认为具有一定的 HVS 特性且好于 *PSNR* 和 *MSE* 的指标. 作为比较,表 2 给出了文献[1]的实验结果,从表 1 和表 2 给出的结果来看,本文所提出的算法的综合性能要高于 Wu 的方法.

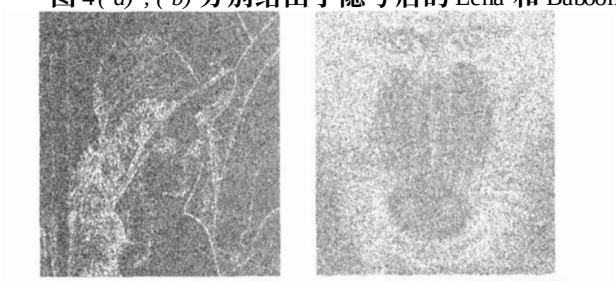
表 1 本文方案的实验结果

测试图像	容量(比特/像素)	*wPSNR*(dB)	*PSNR*(dB)	*mssim*
Lena	1.6655	44.4323	42.2624	0.9742
Baboon	2.0279	45.2742	38.3523	0.9836
peppers	1.7286	43.9125	41.3812	0.9736
Jet	1.6945	44.9119	41.6052	0.9769

表 2 文献[1]的实验结果

测试图像	容量(比特/像素)	*wPSNR*(dB)	*PSNR*(dB)	*mssim*
Lena	1.5256	44.8804	42.7973	0.9759
Baboon	1.7632	44.9961	36.1802	0.9823
peppers	1.5313	44.9428	41.9258	0.9786
Jet	1.5598	44.5001	40.4829	0.9730

图 4(*a*),(*b*)分别给出了隐写后的 Lena 和 Baboon 以 40 倍增强了的载体图像和隐写图像的差分图像. 从图中可以看出,隐写产生的修改多数发生在边缘和纹理较强的区域,而这些区域具有更好的视觉掩蔽效应.



(*a*) Lena隐写后的增强差分图像 (*b*) Baboon隐写后的增强差分图像

图4 实验结果

5 结论

为实现感知质量和容量之间的更好折衷,本文提出一种基于量化的自适应隐写机制,该机制通过设计具有 HVS 特征的分割码本实现将不同数量的消息比特嵌入到图像具有不同视觉敏感特性的区域中,并被用于图像三像素组的数据嵌入中. 实验表明该方案在容量和感知质量方面具有较好的综合性能. 在进一步的研究中,将考虑利用这一机制实施 JPEG 图像的隐写. 此外,需要说明的是本文仅关注容量和感知质量指标,对安全性的问题未加考虑,因此在将安全性问题考虑进来并引入统计保持的嵌入策略,可提供既安全且容量高失真低的隐写方案,这也是我们未来的研究方向.

作者简介:

戴跃伟 男,1962 年 10 月出生于江苏镇江,教授,博士生导师. 研究领域为信息安全的理论与技术、系统工程、随动系统技术与应用等.
Email:daiywei@163.com

刘光杰 男,1980 年 2 月出生于江苏徐州,博士,讲师. 2002 年和 2007 年在南京理工大学获得工学学士和工学博士学位. 主要研究方向为信息隐藏、数据认证等.
Email:guangj_liu@yahoo.com.cn

参考文献:

[1] WU D C, Tsai W H. A steganographic method for images by pixelvalue differencing[J]. Pattern Recognition Letters, 2003, 24(9-10):1613-1626.

[2] MING C, WU N I. A high quality steganographic method with pixelvalue differencing and modulus function[J]. Journal of Systems and Software, 2008, 81(1):150-158.

[3] C C Chang, H W Tseng. A steganographic method for digital images using side match[J]. Pattern Recognition, 2004, 25(12):1431-1437.

(下转第 24 页)

[9] T Sturm, J von Voss, M Boger. Generating code from UML with velocity templates[J]. The Unified Modeling Language. 2002, 2460: 379 - 386.

作者简介:

冯锦丹 女, 1980 年生于辽宁锦州. 哈尔滨工业大学计算机科学与技术学院博士生, 研究方向为软件复用、软构件与代码生成.
E-mail: fjd1127@163.com

战德臣 男, 博士, 教授, 博士生导师, CCF 高级会员. 主要研究领域为软件复用与软件体系结构、模型驱动架构、现代企业管理、数据与知识工程.
E-mail: dechen@hit.edu.cn

聂兰顺 男, 博士, 讲师, 主要研究领域为软件体系结构、软件复用、大型管理软件.

徐晓飞 男, 院长, 博士, 教授, 博士生导师, CCF 高级会员. 主要研究领域为管理与决策信息系统、数据库、企业资源计划与供应链管理技术、服务科学.

(上接第 38 页)

[4] LIU G J, WANG J W, et al. Data hiding in neural network predictioni errors[A], Lecture Notes in Computer Scence (Advances in Neural Networks-ISNN 2006)[C], Heidelbergpp: Springer Berlin, 2006. 273 - 278.

[5] PARK Y-R, KANG H-H, et al. A steganographic scheme in digital images using information of neighboring pixels[A]. Lecture Notes in Computer Scence (Advances in Natural Computation)[C]. Heidelbergpp: Springer Berlin, 2005. 962 - 967.

[6] PARK Y-R, KANG H-H, et al. An image steganography using pixel characteristics[A]. Lecture Notes in Artificial Intelligence (Computational Intelligence and Security)[C]. Heidelbergpp: Springer Berlin, 2005. 581 - 588.

[7] ZHANG X P, WANG S Z, Steganography using multiple-base notational system and human vision sensitivity[J]. IEEE Signal Processing Letters, 2005, 12(1): 67 - 70.

[8] YANG C Y, LIN J C, Image hiding by base-oriented algorithm [J]. Optical Engeering, 2006, 45(11): 117001 - 1 - 117001 - 10.

[9] WESTFELD A. Space filling curves in steganalysis[A]. Proccedings of SPIE: Security, Steganography and Watermarking for Multimedia[C]. San Jose, California: SPIE, 2005. 28 - 37.

[10] VOLOSHYNOVSHIY S, PEREIRA S, et al. Attacking modelling: towards a second generation watermarking benckmark [J]. Signal Processing, 2001, 81(6): 1177 - 1214.

[11] WANG Z, BOVIK A C, et al. Image quality assessment: From error visibility to structural similarity[J]. IEEE Transaction on Image Processing, 2004, 13(4): 600 - 612.