计算机研究与发展
Journal of Computer Research and Development
ISSN 1000-1239/CN 11-1777/TP
49(8): 1668-1675, 2012

# 基于隐写编码和 Markov 模型的自适应图像隐写算法

张 湛[1,2] 刘光杰[1] 戴跃伟[1] 王执铨[1]
[1](南京理工大学自动化学院 南京 210094)
[2](重庆电子工程职业学院计算机应用系 重庆 401331)
(zhang_zhan_zz@126.com)

# A Self-Adaptive Image Steganography Algorithm Based on Cover-Coding and Markov Model

Zhang Zhan[1,2], Liu Guangjie[1], Dai Yuewei[1], and Wang Zhiquan[1]
[1](*School of Automation, Nanjing University of Science and Technology, Nanjing* 210094)
[2](*Department of Computer Application, Chongqing College of Electronic Engineering, Chongqing* 401331)

**Abstract** It is a difficulty and hotspot how to desigh steganography algorithms with large-capacity, low-distortion and high statistical security. A self-adaptive image steganography algorithm which takes account of the perceptual distortion and second-order statistical security is proposed. It introduces the smoothness of the various parts of the cover-object to the encoding generation process of cover codes, and reduces the distortion by the reasonable use of a cluster of cover codes in each part of cover-object. In the embedding aspect, in order to improve the statistic security, the algorithm uses a dynamic compensate method based on the image Markov chain model, and it embeds secret information into the least two significant bit (LTSB) planes in order to ensure the capacity. Experiment results show the proposed algorithm has lower distortion and smaller changes of cover statistical distribution than the stochastic LTSB match steganography algorithm and the algorithm which only uses one cover code under the same embedded payload. And the proposed algorithm has larger payloads than one cover code embedding when the distortion and statistical distribution changes are close.

**Key words** information hiding; steganography; cover code; Markov chain; steganography security

**摘 要** 如何构造大容量、低失真和高统计安全的隐写算法一直是隐写研究的难点和热点.提出一种兼顾感知失真和二阶统计安全的自适应图像隐写算法设计思路.算法将载体各部分的平滑度引入隐写编码的生成过程,自适应地利用一簇隐写编码在载体各部分的合理运用降低载密图像失真度;在隐秘信息嵌入方式上利用基于 Markov 链模型的动态补偿方法提高载密图像统计安全性;算法对载体最低有效位和次最低有效位进行嵌入以保证嵌入容量.实验表明算法在相同嵌入量下相较双层随机 LSB 匹配算法以及仅使用一种隐写编码的算法,失真度更低且载体统计分布的改变更小,而在失真度和统计分布改变相近时嵌入容量更大.

**关键词** 信息隐藏;隐写;隐写编码;Markov 链;隐写安全

**中图法分类号** TP309



**收稿日期**:2010-04-21;**修回日期**:2012-02-06
**基金项目**:江苏省自然科学基金项目(BK2008403)

隐写术是信息安全研究领域中的一个重要分支,其本质就是将秘密信息隐藏在可公开传输的载体中,从而利用公共信道实现隐秘通信.近年来,随着隐写分析技术的迅速发展[1],人们对隐写系统性能的要求不断提高,设计满足隐写三要素(高容量、低感知失真和高统计安全)的隐写算法已成为隐写术发展的迫切诉求.

低感知失真图像隐写算法的核心思想是在保证较大嵌入量的前提下取得较好保真度.这类算法大多基于图像局部复杂度的方法:如 Wu 等人提出的在图像值差中隐藏信息的方法[2],该方法利用了具有较大差值图像局部能容纳较多信息的特性;Liu 等人提出一种基于神经网络预测误差的隐写算法[3],将数据嵌入图像预测误差域中;Ming 等人通过引入模函数改进了文献[2]的方法[4],取得了更大嵌入容量.另外其他许多研究者也提出了不同的低失真隐写算法[5-6].

高统计安全图像隐写算法的核心思想则是在保证较大容量的基础上减小载密图像和载体图像的统计分布距离,使得隐写分析的"显微镜"不能检测出载密图像,从而提高隐秘通信的安全性.早期安全隐写术主要针对专用隐写分析方法[7-9].当前主流的做法是降低修改量的隐写编码方法,和维持隐写前后统计特性不发生较大变化的统计保持方法.隐写编码技术可在降低隐写容量的前提下提高隐写效率,即对载体作尽量少的修改而隐藏尽可能多的消息,进而大幅降低隐写引起的载体失真并提高隐写安全性.Fridrich 等人在线性编码和单一编码系统中讨论了隐写编码的问题[10];Mielikainen 则基于 Hamming 码提出三元隐写编码[11];另外文献[12-15]也从不同角度研究了各种隐写编码.当前多数基于统计特性保持的安全隐写算法主要集中在一阶统计特性——直方图分布的保持上[16-17].最近也有研究者开始讨论高阶统计特性的保持问题:如 Sarkar 等人提出使用部分图像分块 DCT 变换系数对嵌入时统计特性的改变进行补偿的二阶保持隐写算法[18];张湛等人[19]则利用图像 Markov 链(Markov chain,MC)模型统计测度优化嵌入器,从而提高载密图像二阶统计安全性.

上述文献对各种隐写算法的研究大多是在考虑隐写三要素中的两个要素的基础上进行的.为在保持隐写容量的同时降低载体感知失真,多数文献利用视觉掩蔽效应,基于图像局部复杂度的变化进行嵌入操作,并取得了较好的效果.因为载体统计安全性是针对载体整体统计特性的要素,所以许多文献在保持较大隐写容量的前提下从载体整体统计分布考虑,采用各种优化或补偿方法进行嵌入操作,亦取得了许多显著成果.由于隐写算法的性能主要由其三要素共同决定,因此如何综合考虑三要素,既利用载体局部特性以改善载体感知失真,又着眼于载体整体统计分布以增强其安全性,在保证较大嵌入容量基础上使得载密载体失真度更小、统计分布保持更好,有着实际的研究价值.

本文综合考虑载体感知失真和统计分布的改变,在保证一定容量的基础上提出一种低失真的二阶统计安全隐写算法.该算法对载体图像分块,将各图像块的平滑度引入隐写编码生成过程,自适应地生成针对不同平滑度图像块的隐写编码以降低感知失真;在隐秘信息嵌入过程中利用基于图像 MC 模型的动态补偿方法提高载密图像的二阶统计安全性;对载体最底层的两个位平面(least two significant bit, LTSB)进行嵌入以保证嵌入容量.实验表明在相同嵌入量情况下,该算法比随机 LTSB 匹配算法以及仅使用一种隐写编码的算法,感知失真度更低且载体统计分布的改变更小;而在载体失真度和统计分布的改变相近的情况下,该算法比仅使用一种隐写编码的算法嵌入容量更大.

## 1　自适应隐写编码和二阶动态补偿嵌入方式

本节首先简要介绍将图像块平滑度引入隐写编码方式中,构造与图像各部分自适应的隐写编码的方法,并利用该方法改善载密图像的感知失真,进而简述利用图像 MC 模型的经验矩阵将隐秘信息以动态补偿的方式嵌入载体中,以改善载密图像的二阶统计安全性的方法.

### 1.1　基于图像块平滑度的自适应隐写编码

通常自然图像各部分像素平滑度存在差异,且不同部分的差异有时非常大,当改变自然图像不同的部分以嵌入隐秘信息时,其对载体感知失真度的影响也各不相同.一般图像的纹理较强,即平滑度较低的部分具有较好的视觉掩蔽效应,在图像平滑度较高部分嵌入较少隐秘信息,反之嵌入较多隐秘信息可以使得载密图像获得更好的视觉保真度.因此,可根据图像各部分平滑度自适应地决定其应承载的隐秘信息量,并使用隐写编码的方式降低对该部分嵌入的载体像素改动量,使得载密图像感知失真更低且在一定程度上提高隐秘信息的安全性能.

由于张新鹏等人提出的基于稀疏表示的编码方法[14]可产生固定待嵌载体序列长度 $n$ 和嵌入信息量 $r$ 的隐写编码 $C(n,r)$,$(\mathrm{lb}(n+1)\leqslant r\leqslant n)$(此处和下面均以 $C(n,r)$ 代表一种编码方法),且实现方法简单,易于应用,因此本文根据载体图像块(包含 $n$ 个载体像素)平滑度计算其嵌入量 $r$,并利用该编码方法生成对应的隐写编码以降低载密图像的感知失真.

设大小为 $M_B\times N_B=n$ 的灰度图像块为 $\boldsymbol{B}(i,j)$,则 $\partial\boldsymbol{B}/\partial i$ 和 $\partial\boldsymbol{B}/\partial j$ 分别为 $\boldsymbol{B}(i,j)$ 沿 $i$ 和 $j$ 方向的梯度. 由于数字图像像素为整数,$\partial\boldsymbol{B}/\partial i$ 和 $\partial\boldsymbol{B}/\partial j$ 可使用差分 $\Delta_i=\boldsymbol{B}(i+1,j)-\boldsymbol{B}(i,j)$ 和 $\Delta_j=\boldsymbol{B}(i,j+1)-\boldsymbol{B}(i,j)$ 近似,则该图像块的像素平滑度 $\xi$ 可表示为

$$\xi\triangleq\frac{1}{2}\left(\sum_{i=1}^{M_B}\sum_{j=1}^{N_B-1}|\Delta_i|+\sum_{j=1}^{N_B}\sum_{i=1}^{M_B-1}|\Delta_j|\right). \tag{1}$$

通常若 $\xi$ 较大,则 $\boldsymbol{B}$ 可承载较多隐秘信息且对图像失真度影响较小,因此可根据 $\xi$ 计算与 $\boldsymbol{B}$ 相适应的嵌入量 $r$. 设:

$$\bar{r}=\begin{cases}0, & \xi=0;\\ [2\times\ln\xi], & \xi\neq 0,\end{cases} \tag{2}$$

其中[·]为四舍五入取整. 则:

$$r=\begin{cases}0,\bar{r}\leqslant 2;\\ \mathrm{lb}(n+1), & 2<\bar{r}<\mathrm{lb}(n+1);\\ \bar{r}, & \mathrm{lb}(n+1)\leqslant\bar{r}\leqslant n;\\ n, & \bar{r}>n.\end{cases} \tag{3}$$

当待嵌载体图像块的大小 $n$ 确定后,利用式(1)~(3)计算该图像块的隐秘信息嵌入量 $r$,进而提取 $r$ 比特的隐秘信息,利用文献[14]的方法生成该图像块的隐写编码 $C_B(n,r)$,从而得到嵌入时在 $\boldsymbol{B}$ 中的改变位置.

### 1.2 基于 MC 模型的动态补偿嵌入方式

由于载体图像的统计分布是对整幅图像的统计,因此改变图像块相应位置以嵌入隐秘信息时,必须从载体图像的整体统计分布的变化考虑,以决定每一次改变的改动方式(如对载体 LSB 位嵌入时可采用 $\pm1$ 等改动方式).

Sullivan 等人在文献[20]中详细论述了图像 MC 模型及其经验矩阵的构造,进而张湛等人在文献[19]中证明了该模型二阶统计分布保持与 Cachin 提出的一阶统计分布保持的一致性[21]. 因此在隐秘数据嵌入时可以 MC 模型为指导,降低载密图像的二阶统计分布的改变,从而提高隐秘信息的统计安全性. 由于文献[20]中提出的图像隐写 MC 模型二阶安全性指标的计算较为复杂,若采用类似文献[19]中的方法,直接使用 MC 模型指导每一比特信息的嵌入,必然导致隐写过程的巨大运算量,不利于大量隐写载体的嵌入. 考虑到通常经过加密的待嵌隐秘信息具有 0-1 均匀分布的特性,因此可在对每一次嵌入操作时,记录其引起的载体 MC 模型经验矩阵的改变,控制嵌入器利用后期嵌入操作补偿前期嵌入对载体二阶统计分布的改变,即利用动态补偿的方式,在不降低嵌入量且根本不进行 MC 模型二阶安全性指标的计算的情况下,使载体统计特性尽可能保持,且极大地提高隐写嵌入的速度,更加适合大容量隐写的应用.

设载体图像经验矩阵为 $\boldsymbol{G}$,分析其构成[20]可知,若改变 MC 中某一位 $x_k$($k=1,2,\cdots,l$,$l$ 为 MC 链长),必然影响 $\boldsymbol{G}$ 的 4 个位. 其中两位增加数值 $1/(l-1)$,另两位减少 $1/(l-1)$. 设 $\boldsymbol{G}$ 的序号计数从 1 开始,以 8 位灰度图像为例,若 $x_k$ 位数值增加或减小 1(即改变 $x_k$ 的最低位),则 $\boldsymbol{G}(x_{k+1}+1,x_k+1)$ 与 $\boldsymbol{G}(x_k+1,x_{k-1}+1)$ 位数值减小 $1/(l-1)$,而 $\boldsymbol{G}(x_{k+1}+1,x_k+2)$ 与 $\boldsymbol{G}(x_k+2,x_{k-1}+1)$ 或 $\boldsymbol{G}(x_{k+1}+1,x_k)$ 与 $\boldsymbol{G}(x_k,x_{k-1}+1)$ 位数值增加 $1/(l-1)$;同样若 $x_k$ 位数值增加或减小 2(即改变 $x_k$ 的次最低位),则 $\boldsymbol{G}(x_{k+1}+1,x_k+1)$ 与 $\boldsymbol{G}(x_k+1,x_{k-1}+1)$ 位数值减小 $1/(l-1)$,而 $\boldsymbol{G}(x_{k+1}+1,x_k+3)$ 与 $\boldsymbol{G}(x_k+3,x_{k-1}+1)$ 或 $\boldsymbol{G}(x_{k+1}+1,x_k-1)$ 与 $\boldsymbol{G}(x_k-1,x_{k-1}+1)$ 位数值增加 $1/(l-1)$.

因此可设置标志矩阵 $\boldsymbol{F}_{256\times256}$. $\boldsymbol{F}$ 中的每一个元素与 $\boldsymbol{G}$ 一一对应,且初始为零矩阵. 若 $\boldsymbol{G}$ 的位发生变化,则 $\boldsymbol{F}$ 对应位也相应变化. 即若 $\boldsymbol{G}$ 的某位增加(或减小)$1/(l-1)$,则 $\boldsymbol{F}$ 对应位增加(或减小)1. 如此,$\boldsymbol{F}$ 的变化可直观反映出由于载体图像嵌入数据后 $\boldsymbol{G}$ 所发生的变化. 若能完全补偿二阶统计分布,则 $\boldsymbol{F}$ 最终应为零矩阵.

## 2 基于隐写编码和 MC 模型的自适应图像隐写算法

本节以 8 位灰度图像 $\boldsymbol{A}$ 为例,将 $\boldsymbol{A}$ 分成幅面为 $M_B\times N_B=n$ 的互不相交的图像块 $\boldsymbol{B}_t$,$t$ 表示图像块在 $\boldsymbol{A}$ 中的位置. 在不同 $\boldsymbol{B}_t$ 中嵌入隐秘信息的操作对 $\boldsymbol{A}$ 的感知失真影响不同,根据 $\boldsymbol{B}_t$ 的平滑度 $\xi_t$ 的大小计算 $\boldsymbol{B}_t$ 的嵌入量 $r_t$,并根据文献[14]的方法生成 $\boldsymbol{B}_t$

的隐写编码 $C_{\boldsymbol{B}_t}(n,r_t)$,最后基于 $\boldsymbol{A}$ 的 MC 模型,利用动态补偿的嵌入方式将隐秘信息嵌入 $\boldsymbol{B}_t$ 中,从而得到低失真高统计安全的载密图像.

### 2.1　符号定义

定义大小为 $M\times N$ 的 8 位灰度图像 $\boldsymbol{A}$,$\boldsymbol{G}$ 为 $\boldsymbol{A}$ 的 MC 经验矩阵,$x_k$ 为 $\boldsymbol{A}$ 中像素,$k$ 为该像素在 $\boldsymbol{A}$ 的 MC 中位置,$x_k\in[0,255]$. 定义 $\boldsymbol{B}_t$ 为 $\boldsymbol{A}$ 所分成的互不相交 $M_{\boldsymbol{B}}\times N_{\boldsymbol{B}}$ 图像块($M_{\boldsymbol{B}}\times N_{\boldsymbol{B}}=n$),$t$ 为块序号,$\boldsymbol{E}_t$ 为 $\boldsymbol{B}_t$ 像素次最低有效位层数据按照某种方式排列成的待嵌载体向量,$\widetilde{\boldsymbol{B}}_t$ 为 $\boldsymbol{B}_t$ 对应的载密图像块,$\xi_t$ 为 $\boldsymbol{B}_t$ 的像素平滑度. 定义 $\boldsymbol{B}_t^{\mathrm{L}}$ 为 $\boldsymbol{B}_t$ 左方相邻块,$\boldsymbol{B}_t^{\mathrm{U}}$ 为 $\boldsymbol{B}_t$ 上方相邻块,$\boldsymbol{B}_t^{\mathrm{LU}}$ 为 $\boldsymbol{B}_t$ 左上方相邻块,像素平滑度分别为 $\xi_t^{\mathrm{L}}$,$\xi_t^{\mathrm{U}}$,$\xi_t^{\mathrm{LU}}$,$\hat{\xi}_t$ 为根据 $\xi_t^{\mathrm{L}}$,$\xi_t^{\mathrm{U}}$ 和 $\xi_t^{\mathrm{LU}}$ 预测的 $\boldsymbol{B}_t$ 像素复杂度. 定义 $r_t$ 为 $\boldsymbol{B}_t$ 的嵌入量,$C_{\boldsymbol{B}_t}(n,r_t)$ 为 $\boldsymbol{B}_t$ 对应的隐写编码,即根据像素平滑度生成的、在大小为 $n$ 的载体像素块 $\boldsymbol{B}_t$ 中嵌入长度为 $r_t$ 的隐秘信息时所使用的隐写编码. 定义经加密后的待嵌隐秘信息比特序列为 $\boldsymbol{S}=\{s_1,s_2,\cdots,s_m\}$,$m$ 为序列长度. 定义经过 LSB 层嵌入操作的载体像素为 $\hat{x}_k$,而 $\hat{x}_k$ 经过 LTSB 层嵌入改动后的载体像素为 $\tilde{x}_k$.

定义函数 $\Lambda_{+1}$,$\Lambda_{-1}$,$\Lambda_{+2}$,$\Lambda_{-2}$ 和 $\Lambda_0$ 分别表示对像素值作 $+1$,$-1$,$+2$,$-2$ 操作和不操作. 函数 $L_1(x)$ 和 $L_2(x)$ 分别为提取像素 $x$ 的最低位(least significant bit, LSB)和次最低位.

### 2.2　隐写算法

首先设定嵌入函数 $\Gamma_1$,$\Gamma_2$,$\Gamma_3$,$\Gamma_4$,$\Gamma_5$,$\Gamma_6$ 如下(其中 $s_i$ 为待嵌信息):

$$\Gamma_1(x_k,s_i)=\begin{cases}\Lambda_0(x_k),\ L_1(x_k)=s_i;\\ \Lambda_{+1}(x_k),\ L_1(x_k)\neq s_i,\\ \quad x_k\in[0,255);\\ \Lambda_{-1}(x_k),\ L_1(x_k)\neq s_i,x_k=255;\end{cases}\tag{4}$$

$$\Gamma_2(x_k,s_i)=\begin{cases}\Lambda_0(x_k),\ L_1(x_k)=s_i;\\ \Lambda_{-1}(x_k),\ L_1(x_k)\neq s_i,\\ \quad x_k\in(0,255];\\ \Lambda_{+1}(x_k),\ L_1(x_k)\neq s_i,x_k=0;\end{cases}\tag{5}$$

$$\Gamma_3(x_k,s_i)=\begin{cases}\Lambda_0(x_k),\ L_1(x_k)=s_i;\\ \text{随机选择 }\Lambda_{-1}(x_k)\text{ 或 }\Lambda_{+1}(x_k),\\ \quad L_1(x_k)\neq s_i,x_k\in(0,255);\\ \Lambda_{+1}(x_k),\ L_1(x_k)\neq s_i,x_k=0;\\ \Lambda_{-1}(x_k),\ L_1(x_k)\neq s_i,x_k=255;\end{cases}\tag{6}$$

$$\Gamma_4(x_k)=\begin{cases}\Lambda_{+2}(x_k),\ x_k\in[0,254);\\ \Lambda_{-2}(x_k),\ x_k\in[254,255];\end{cases}\tag{7}$$

$$\Gamma_5(x_k)=\begin{cases}\Lambda_{-2}(x_k),\ x_k\in(1,255];\\ \Lambda_{+2}(x_k),\ x_k\in[0,1];\end{cases}\tag{8}$$

$$\Gamma_6(x_k)=\begin{cases}\text{随机选择 }\Lambda_{-2}(x_k)\text{ 或 }\Lambda_{+2}(x_k),\\ \quad x_k\in(1,254);\\ \Lambda_{+2}(x_k),\ x_k\in[0,1];\\ \Lambda_{-2}(x_k),\ x_k\in[254,255].\end{cases}\tag{9}$$

式(7)~(9)为载体向量和待嵌信息向量经隐写编码后,对需改动像素的次最低位的改动操作. 分别针对载体 LSB 层和次最低位层设定嵌入器 $\Gamma_1^*$ 和 $\Gamma_2^*$ 如下:

$$\Gamma_1^*(x_k,s_i,\boldsymbol{F})=\begin{cases}\Gamma_1(x_k,s_i),\ \boldsymbol{F}(x_{k+1}+1,x_k)>\\ \quad\boldsymbol{F}(x_{k+1}+1,x_k+2);\\ \Gamma_2(x_k,s_i),\ \boldsymbol{F}(x_{k+1}+1,x_k)<\\ \quad\boldsymbol{F}(x_{k+1}+1,x_k+2);\\ \Gamma_3(x_k,s_i),\ \boldsymbol{F}(x_{k+1}+1,x_k)=\\ \quad\boldsymbol{F}(x_{k+1}+1,x_k+2);\end{cases}\tag{10}$$

$$\Gamma_2^*(x_k,\boldsymbol{F})=\begin{cases}\Gamma_4(x_k),\ \boldsymbol{F}(x_{k+1}+1,x_k-1)>\\ \quad\boldsymbol{F}(x_{k+1}+1,x_k+3);\\ \Gamma_5(x_k),\ \boldsymbol{F}(x_{k+1}+1,x_k-1)<\\ \quad\boldsymbol{F}(x_{k+1}+1,x_k+3);\\ \Gamma_6(x_k),\ \boldsymbol{F}(x_{k+1}+1,x_k-1)=\\ \quad\boldsymbol{F}(x_{k+1}+1,x_k+3).\end{cases}\tag{11}$$

由于在本算法中隐写编码主要是为了控制载密图像的感知失真,而在载体 LSB 中嵌入信息比特时,采用 $\Lambda_{+1}$ 和 $\Lambda_{-1}$ 均只会对载体像素造成数值为 1 的微小改动,对载体失真的影响不大(通常在载体 LSB 满嵌入时峰值信噪比(peak signal to noise ratio, PSNR)可达到 51 以上),考虑到采用隐写编码会降低嵌入容量的实际问题,对载体的 LSB 层仅使用嵌入器 $\Gamma_1^*$ 进行嵌入操作,不进行隐写编码操作.

当在载体次最低位层中嵌入信息比特时,由于嵌入器 $\Gamma_2^*$ 对载体改动较大,为控制载密图像的感知失真,需要根据载体各图像块 $\boldsymbol{B}_t$ 的平滑度自适应地产生相应的隐写编码. 由于在 $\boldsymbol{B}_t$ 中嵌入 $\boldsymbol{S}$ 会改变 $\xi_t$,若直接使用 $\xi_t$ 计算 $r_t$,从而生成 $C_{\boldsymbol{B}_t}(n,r_t)$ 可能影响接收方收取信息的正确率. 注意到通常 $\xi_t$ 与相邻块平滑度接近,因此在隐写时可根据 $\boldsymbol{B}_t$ 的预测复杂度 $\hat{\xi}_t$ 指导嵌入. 当 $\boldsymbol{B}_t$ 为第 1 行块时,$\hat{\xi}_t=\xi_t^{\mathrm{L}}$;当 $\boldsymbol{B}_t$ 为第 1 列块时,$\hat{\xi}_t=\xi_t^{\mathrm{U}}$;其他情况下 $\hat{\xi}_t$ 可通过式(12)计算.

$$\hat{\xi}_t=\begin{cases}\min(\xi_t^{\mathrm{L}},\xi_t^{\mathrm{U}}), & \xi_t^{\mathrm{LU}}\geqslant\max(\xi_t^{\mathrm{L}},\xi_t^{\mathrm{U}});\\ \max(\xi_t^{\mathrm{L}},\xi_t^{\mathrm{U}}), & \xi_t^{\mathrm{LU}}\leqslant\min(\xi_t^{\mathrm{L}},\xi_t^{\mathrm{U}});\\ \xi_t^{\mathrm{L}}+\xi_t^{\mathrm{U}}-\xi_t^{\mathrm{LU}}, & \text{其他}.\end{cases}\quad(12)$$

由于本算法是对隐写三要素的综合考虑,具体实现时涉及因素较多,为表述清晰,在图 1 中给出算法流程的简明示意图,其中虚框表示循环:

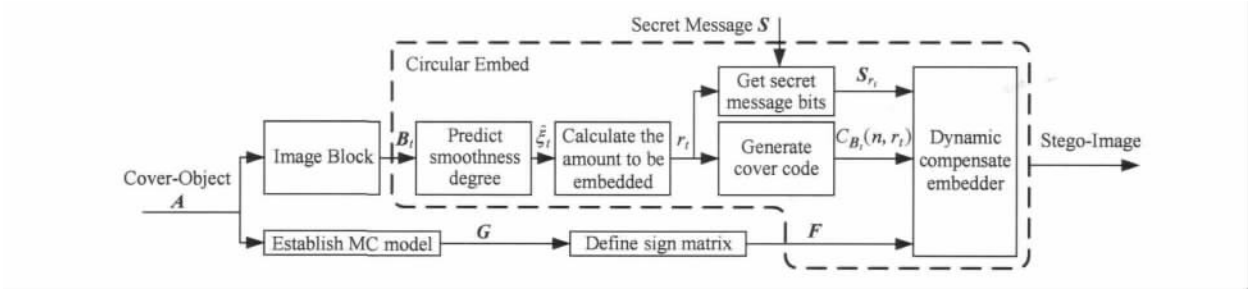


Fig. 1 Flow chart of proposed algorithm.

**图 1 本文算法流程图**

隐写算法具体嵌入步骤如下:

1) 建立载体图像 $A$ 的 MC 模型,并定义与其经验矩阵 $G$ 对应的标志矩阵 $F$;

2) 利用嵌入器 $\Gamma_1^*$ 将 $S$ 中的前 $M\times N$ 比特信息嵌入 $A$ 的 LSB 层中,并在每次嵌入操作时根据 1.2 节的分析将 $G$ 所发生的变化记录在 $F$ 中,以便后续嵌入时根据 $F$ 进行补偿,即 $\hat{x}_k=\Gamma_1^*(x_k,s_i,\boldsymbol{F})$;

3) 根据 $n$ 对已在 LSB 层进行嵌入的载体进行互不相交分块划分,每一分块 $\boldsymbol{B}_t$ 含像素总数 $n$,利用函数 $L_2(\hat{x}_k)$ 提取载体分块 LTSB 层数据,按某种方式(可由密钥确定)排列为待嵌载体向量 $\boldsymbol{E}_t$;

4) 对 $A$ 左上角分块 $\boldsymbol{B}_t$,采用与接收者约定的编码 $\mathrm{C}(n,r)$,在 $S$ 中提取未嵌入的 $r$ 比特信息,根据 $\mathrm{C}(n,r)$ 确定 $\boldsymbol{E}_t$ 的改动位置,将隐秘信息嵌入该分块的次最低位层中,得到载密图像块 $\widetilde{\boldsymbol{B}}_t$;

5) 若 $\boldsymbol{B}_t$ 为载体第 1 行(列)分块,对已完成嵌入的左(上)方图像块 $\widetilde{\boldsymbol{B}}_t^{\mathrm{L}}(\widetilde{\boldsymbol{B}}_t^{\mathrm{U}})$,根据式(1)计算 $\xi_t^{\mathrm{L}}(\xi_t^{\mathrm{U}})$ 并预测 $\hat{\xi}_t$,进而根据式(2)(3)计算 $\boldsymbol{B}_t$ 对应的嵌入量 $r_t$,然后利用文献[14]的方法产生 $\mathrm{C}_{\boldsymbol{B}_t}(n,r_t)$,在 $S$ 中提取未嵌入的 $r_t$ 比特信息,根据 $\mathrm{C}_{\boldsymbol{B}_t}(n,r_t)$ 确定 $\boldsymbol{E}_t$ 的改动位置,将隐秘信息嵌入该分块的次最低位层中得到 $\widetilde{\boldsymbol{B}}_t$;

6) 若 $\boldsymbol{B}_t$ 不属于载体第 1 行或第 1 列分块,则根据式(12)预测 $\hat{\xi}_t$,进而根据式(2)(3)计算 $\boldsymbol{B}_t$ 对应的嵌入量 $r_t$,然后利用文献[14]的方法产生 $\mathrm{C}_{\boldsymbol{B}_t}(n,r_t)$,在 $S$ 中提取未嵌入的 $r_t$ 比特信息,根据 $\mathrm{C}_{\boldsymbol{B}_t}(n,r_t)$ 确定 $\boldsymbol{E}_t$ 的改动位置,将隐秘信息嵌入该分块的次最低位层中得到 $\widetilde{\boldsymbol{B}}_t$;

7) 在步骤 4)~6)嵌入时,对于需改动像素的操作.按照该像素在载体 MC 中的位置,参考 $F$ 的变化情况,利用嵌入器 $\Gamma_2^*$ 进行嵌入操作,即对需改动的像素 $\widetilde{x}_k=\Gamma_2^*(\hat{x}_k,\boldsymbol{F})$.为保证嵌入过程完成后 $|x_k-\widetilde{x}_k|\leqslant 2$,比较 $x_k$ 与 $\widetilde{x}_k,\hat{x}_k$ 由式(13)确定:

$$\widetilde{x}_k=\begin{cases}x_k-1, & x_k-\widetilde{x}_k=-3;\\ x_k+1, & x_k-\widetilde{x}_k=3;\\ \widetilde{x}_k, & x_k-\widetilde{x}_k\in(-3,3).\end{cases}\quad(13)$$

同样在每次改动时根据 1.2 节的分析将 $G$ 所发生的变化记录在 $F$ 中,以便后续嵌入时根据 $F$ 进行补偿.

隐写者与接收者共享编码生成方式、载体分块方式、载体 LSB 层和载体分块的次最低位层的排列方式(可根据密钥得到),并约定载体左上角分块的编码方式.

接收者首先提取载密图像 LSB,得到前 $M\times N$ 比特信息,然后对载密图像分块,将左上角块的次最低位排列为一维向量,并采用约定方式解码得到该块承载的隐秘信息;对其他分块 $\widetilde{\boldsymbol{B}}_t$,首先根据式(12)计算其预测像素平滑度 $\hat{\xi}_t$(第 1 行和第 1 列块分别按照 $\hat{\xi}_t=\xi_t^L$ 和 $\hat{\xi}_t=\xi_t^U$ 计算),并根据 $\hat{\xi}_t$ 利用式(2)(3)计算出 $r_t$,进而根据约定的方式产生 $\mathrm{C}_{\widetilde{\boldsymbol{B}}_t}(n,r_t)$,最后对 $\widetilde{\boldsymbol{B}}_t$ 的次最低位排列解码得到长度为 $r_t$ 的隐秘信息.接收方对所有载密分块次最低位解码,并与已得到的前 $M\times N$ 比特信息合并即得 $S$.

## 3 实验结果

本节以 8 位灰度载体图像和分块大小 $n=15$ 为例,介绍基于隐写编码和 MC 模型的自适应图像隐写算法的实验情况.对 UCID.V2 图像库[22]中 1 338

幅图像,使用本算法、随机 LTSB match 算法(即在载体像素 LSB 层使用随机±1 嵌入,而在次最低位层采用随机±2 的嵌入方式),以及分别采用 C(15,11),C(15,9),C(15,8),C(15,7) 4 种编码的隐写算法,嵌入相同大小的均匀分布隐秘信息(嵌入率从 1.39 bpp 增加至 1.73 bpp).为充分说明本文算法的综合性能,从隐写三要素(载体感知失真、隐写统计安全性和隐写容量)3 方面进行全面比较.

在载体感知保真度方面采用 PSNR,wPSNR(weighted PSNR)和平均 SSIM(structural similarity)进行衡量.载体感知保真度实验结果如图 2 所示:

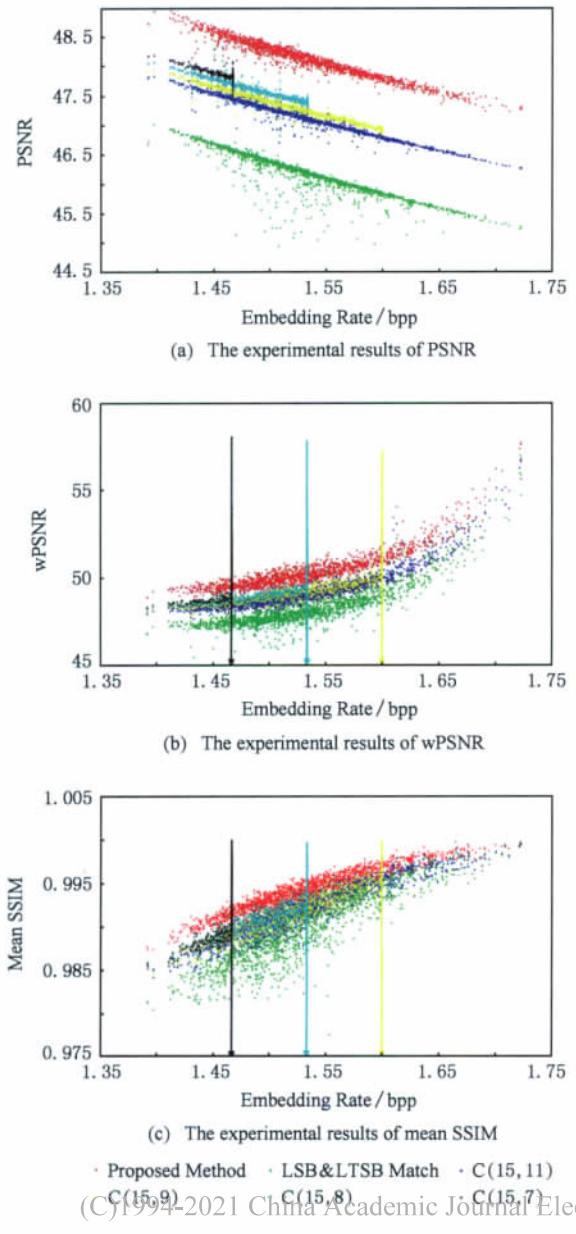


Fig. 2　Experiment results of cover fidelity.

图 2　载体感知保真度实验结果

图 2 的 wPSNR 和平均 SSIM 实验结果中的箭头指示了仅采用一种编码进行隐写的最大嵌入容量.只采用 C(15,11),C(15,9),C(15,8),C(15,7) 4 种编码中的一种进行隐写时的最大嵌入容量分别为 1.73,1.60,1.53 和 1.47 bpp,而本文算法的最大嵌入容量随载体像素复杂度变化,若载体像素复杂度高则最大嵌入容量相较仅采用一种编码的隐写算法更大.在载体保真度方面,采用 C($n$,$r$)一种编码隐写时,随 $r$ 的增加保真度相应降低,而本文算法在相同嵌入量与其余算法比较,保真度有显著提高,并且若保真度相近时本文算法的嵌入容量更大.

在统计安全性方面采用 K-L 散度距离[21](K-L distance)以及 MC 模型二阶散度距离[20](MC distance)进行衡量.实验结果如图 3 所示,为显示清楚,按照随机 LTSB match 的结果从小到大排序且对实验结果纵轴采用对数坐标,在没有超出仅使用一种编码隐写的最大容量时,各种算法在每一幅图像的嵌入容量相同,当已经达到只用一种编码隐写的最大容量后,对于每幅图像本文算法和随机 LTSB match 算法的嵌入容量相同,但均比达到最大容量的那种编码隐写算法更大.

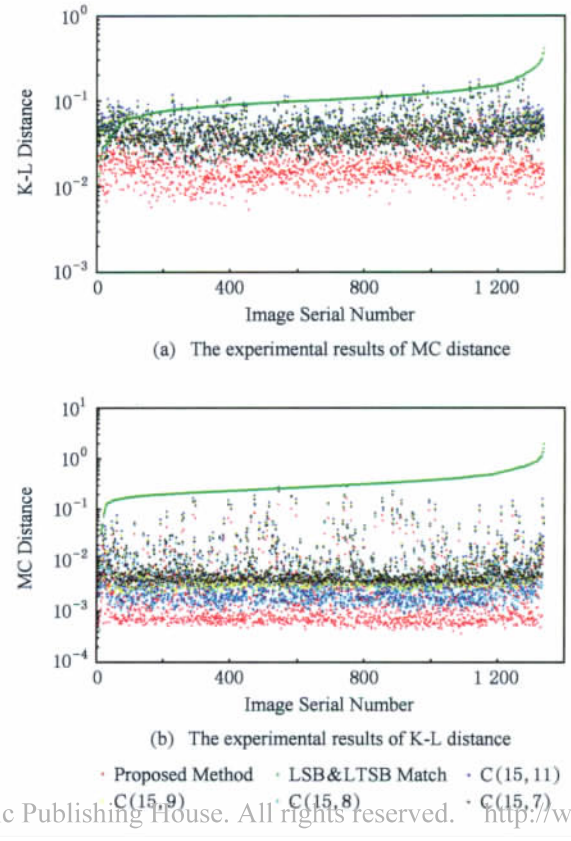


Fig. 3　Experimental results of statistical security.

图 3　统计安全性实验结果

从图 3 可知,对于隐秘信息统计安全性,从 MC distance 和 K-L distance 两方面衡量,本文算法与其余算法比较,统计安全性也是最高的.

图 4 说明了当隐写对载体统计分布的改变相近时,本文算法与仅使用 C(15,11),C(15,9),C(15,8),C(15,7)4 种隐写编码中的一种进行隐写时的嵌入容量比较情况.

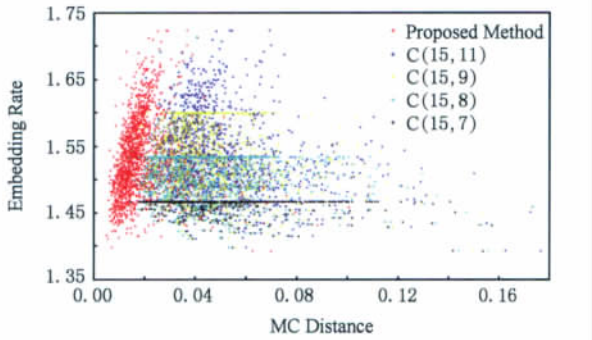


Fig. 4 Experimental results of capacity comparison.

图 4 容量比较实验结果

由图 4 可知,当统计分布的改变相近时,本文算法的嵌入容量较仅使用一种编码进行隐写的算法更高.

## 4 结 论

本文将自适应的隐写编码方式与基于图像 MC 模型的动态补偿嵌入方式相结合,把分块图像像素平滑度引入隐写编码的生成过程,利用自适应的方式对载体像素复杂度较低的部分采用嵌入量较小、对载体改变较少的隐写编码,反之采用嵌入量较大、对载体改变较多的隐写编码嵌入隐秘信息,同时在嵌入操作时采用动态补偿方式以保持载体二阶统计分布,使得隐秘信息在载体不同部分中的分布更符合载体保真度和统计安全性的要求. 实验表明,本文算法在相同嵌入量的情况下比未使用隐写编码的随机 LTSB 匹配算法和仅采用一种隐写编码方式进行隐写的算法,保真度更高且载体统计分布的改变更小. 另一方面,当载体保真度或统计安全性相近时,本文算法比仅采用一种隐写编码进行隐写的算法嵌入容量更大.

由于如今在网络传输的图像中,压缩图像亦占有相当大的比例,因此如何将本文算法的思想推广到压缩图像载体的隐写中以及针对图像变换域的隐写中,设计隐写容量、保真度和统计安全性均有较大提高的隐写算法是进一步研究的方向.

## 参 考 文 献

[1] Wang Shuozhong, Zhang Xinpeng, Zhang Weiming. Recent advances in image-based steganalysis research [J]. Chinese Journal of Computers, 2009, 32(7): 1247-1263 (in Chinese)
(王朔中, 张新鹏, 张卫明. 以数字图像为载体的隐写分析研究进展[J]. 计算机学报, 2009, 32(7): 1247-1263)

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

[3] Liu G J, Wang J W, Lian S G, et al. Data hiding in neural network prediction errors [G] //LNCS 3973: Proc of the 3rd Int Symp on Neural Networks. Berlin: Springer, 2006: 273-278

[4] 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

[5] Dai Yuewei, Liu Guangjie, Ye Shuguang. Adaptive steganography based on Hilbert filling curve [J]. Acta Electronica Sinica, 2008, 36(12A): 24, 35-38 (in Chinese)
(戴跃伟, 刘光杰, 叶曙光. 基于 Hilbert 填充曲线的自适应隐写[J]. 电子学报, 2008, 36(12A): 24, 35-38)

[6] Xu Changyong, Ping Xijian, Liu Cuiqing. Steganography in JPEG encoded images using error-correcting code [J]. Journal of Computer Research and Development, 2009, 46 (Suppl): 132-137 (in Chinese)
(徐长勇, 平西建, 刘翠卿. 利用纠错码的 JPEG 图像压缩域隐写算法[J]. 计算机研究与发展, 2009, 46(增刊): 132-137)

[7] Solanki K, Sarkar A, Manjunath B S. YASS: Yet another steganographic scheme that resists blind steganalysis [G] // LNCS 4567: Proc of the 9th Int Workshop on Information Hiding. Berlin: Springer, 2007: 16-31

[8] Luo W Q, Huang F J, Huang J W. A more secure steganography based on adaptive pixel-value differencing scheme [J]. Multimedia Tools and Applications, 2010, 52 (2/3): 407-430

[9] Liu Wenfen, Guan Wei, Cao Jia, et al. Detection of secret message in spatial LSB steganography based on contaminated data analysis [J]. Journal of Computer Research and Development, 2006, 43(6): 1058-1064 (in Chinese)
(刘文芬, 管伟, 曹佳, 等. 基于污染数据分析实现 LSB 秘密消息的检测[J]. 计算机研究与发展, 2006, 43(6): 1058-1064)

[10] Fridrich J, Soukal D. Matrix embedding for large payloads [J]. IEEE Trans on Information Forensics and Security, 2006, 1(3): 390-395

[11] Mielikainen J. LSB matching revisited [J]. IEEE Signal Processing Letters, 2006, 13(5): 285-287

[12] Zhang X P, Wang S Z. Generalized running coding with prime base for efficient steganographic embedding [J]. Journal of Applied Sciences-Electronics and Information Engineering, 2009, 27(1): 51-55

[13] Zhang W M, Wang S Z, Zhang X P. Improving embedding efficiency of covering codes for applications in steganography [J]. IEEE Communications Letters, 2007, 11(8): 680-682

[14] Zhang Xinpeng, Wang Shuozhong. Steganographic encoding based on sparse representation [J]. Acta Electronica Sinica, 2007, 35(10): 1892-1896 (in Chinese)
(张新鹏, 王朔中. 基于稀疏表示的密写编码[J]. 电子学报, 2007, 35(10): 1892-1896)

[15] Zhang W M, Wang X. Generalization of the ZZW embedding construction for steganography [J]. IEEE Trans on Information Forensics Security, 2009, 4(3): 564-569

[16] Liu G J, Lian S G, Ren Z, et al. Image steganography based on quantization-embedders combination [C] //Proc of the 2007 IEEE Int Conf on Multimedia and Expo, ICME 2007. Piscataway, NJ: IEEE, 2007: 1115-1118

[17] Lu Y F, Li X L, Yang B. A ±1-based steganography by minimizing the distortion of first order statistics [C] //Proc of the 5th Int Conf on Intelligent Information Hiding and Multimedia Signal Processing IIH-MSP 2009. Piscataway, NJ: IEEE, 2009: 60-64

[18] Sarkar A, Solanki K, Manjunath B S. Further study on YASS: Steganogrpahy based on randomized embedding to resist blind steganalysis [C] //Proc of SPIE-The Int Society for Optical Engineering. Bellingham, WA: SPIE, 2008, 6819: 17-28

[19] Zhang Zhan, Liu Guangjie, Wang Junwen, et al. A novel quantization-embedded steganographic algorithm based on Markov chain security [J]. Journal of Optoelectronics · Laser, 2009, 2(7): 944-949 (in Chinese)
(张湛, 刘光杰, 王俊文, 等. 基于 Markov 链安全性的量化隐写算法[J]. 光电子 · 激光, 2009, 2(7): 944-949)

[20] Sullivan K, Madhow U, Chandrasekaran S, et al. Steganalysis for Markov cover data with applications to images [J]. IEEE Trans on Information Forensics and Security, 2006, 1(2): 275-287

[21] Cachin C. An information-theoretic model for steganography [J]. Information and Computation, 2004, 192(1): 41-56

[22] Schaefer G, Stich M. UCID-An uncompressed colour image database [DB/OL]. (2004-12-30) [2010-12-19]. http://vision.cs.aston.ac.uk/datasets/UCID/ucid.html

**Zhang Zhan**, born in 1974. PhD. Lecturer of Chongqing College of Electronic Engineering. His main research interests include information security, steganography and etc.

**Liu Guangjie**, born in 1980. PhD. Associate professor of the School of Automation, Nanjing University of Science and Technology. His main research interests include steganalysis and digital image authentication(Guangj_liu@yahoo.com.cn).

**Dai Yuewei**, born in 1962. PhD. Professor and PhD supervisor of the School of Automation, Nanjing University of Science and Technology. His main research interests include multimedia information security and digital watermarking(daiywei@163.com).

**Wang Zhiquan**, born in 1939. Professor and PhD supervisor of the School of Automation, Nanjing University of Science and Technology. His main research interests include fault-tolerant control and multimedia information security (wangzqwhz@yahoo.com.cn).