n 维超立方体模映射安全隐写算法

廖琪男[1],孙宪波[2],潘瑞冬[3]
(1. 广西财经学院计算机科学系,广西南宁 530003; 2. 广西财经学院应用数学系,广西南宁 530003;
3. 广西财经学院实验中心,广西南宁 530003)

摘 要: 针对目前基于模函数的隐写研究现状,提出 n 维超立方体模映射隐写算法. 根据模运算性质定义一个 n 维模函数,将 n 个像素值映射到一位 a^n 进制数值,从而可以实现将一位 a^n 进制信息隐藏到 n 个像素中. 选择不同的参数 a 可以得到不同的嵌入率和载密图像视觉质量,选择较大的参数 n 且 a 为偶数时可以得到更好的载密图像视觉质量. 理论分析和实验结果表明,本文算法与众多隐写算法相比,不仅具备这些算法的功能,而且具有更好的载密图像视觉质量、安全性和更强的实用性.

关键词: 数字图像; 模函数; 余数循环; 隐写
中图分类号: TP391 **文献标识码:** A **文章编号:** 0372-2112 (2016) 01-0160-08
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2016.01.024

Secure Steganography by n-Dimensional Hypercube Modulo Mapping

LIAO Qi-nan[1], SUN Xian-bo[2], PAN Rui-dong[3]
(1. *Department of Computer Science, Guangxi University of Finance & Economics, Nanning, Guangxi* 530003, *China*;
2. *Department of Applied Mathematics, Guangxi University of Finance & Economics, Nanning, Guangxi* 530003, *China*;
3. *Experimental Center, Guangxi University of Finance & Economics, Nanning, Guangxi* 530003, *China*)

Abstract: In order to solve the problems existing in steganography based on modular function, this paper presents n-dimensional hypercube modulo mapping steganographic algorithm. According to modular arithmetic properties, the algorithm defines an n-dimensional modular function which n pixels values are mapped to a data in a^n-ary notational system, thus the algorithm realizes that each secret digit in a^n-ary notational system is carried by n cover pixels. The algorithm can get different rates of embedding and visual quality of stego image when we choose different parameter a, and can get better visual quality of stego image when a is even number and we choose bigger parameter n. Theoretical analysis and experimental results show that the proposed algorithm, by comparing with many steganography, not only has the function of these algorithms, but also has a better visual quality of stego image, better security, and stronger practicability.

Key words: digital image; modular function; remainder cycle; steganography

1 引言

信息隐藏算法可分为空域算法和频域算法. 在空域隐写算法中,简单有效而又著名的方法就是最低有效位(Least Significant Bit, LSB)取代算法[1],为克服 LSB 容易被图像直方图和 RS(Regular Singular, RS)隐写分析[2]这一缺陷,LSB 匹配算法[3]和动态补偿 LSB 隐写方法[4]等抗 LSB 侦测的隐写算法被提出来. 为提高 LSB 匹配算法的视觉质量,Mielikainen 提出 LSB 匹配重访(LSB Matching Revisited, LSBMR)算法[5]. 为了提高 LSBs (Least Significant Bits, LSBs)视觉质量,Chan 等人提出优化调整像素值(Optimal Pixel Adjustment Process, OPAP)的 LSBs 算法[6]. 目前,LSB 算法仍在信息隐藏占有重要地位,在频域算法中有很多算法采用了 LSB 算法或思想[7~9],以及应用 LSB 结合像素差、像素边缘匹配和图像局部复杂度等的自适应隐写算法[10~12].

2006 年 Zhang 与 Wang 提出利用改变方向(Exploiting Modification Direction, EMD)的模运算隐写算法[13],该方法可以实现将 1 位($2n+1$)进制信息嵌入到 n 个载体像素中,其具有高嵌入效率和良好的载密图像视觉质量,但其最大理论嵌入率只有 1.16 bpp(bits per pixel),故有许多研究者都参考模运算的余数循环特性提出改进

收稿日期: 2014-07-17; **修回日期:** 2015-05-10; **责任编辑:** 李勇锋
基金项目: 广西高校科研项目(No. YB2014342)

式模运算隐写算法[14~21]. 这些算法在嵌入率和效率等方面性能都有了不同程度的提高或改进,但仍存在着信息数制转换中的数据冗余、或嵌入率低、或应用不够灵活广泛、或安全性差等欠缺或不足.

为解决基于模函数的隐写算法中存在的问题,本文提出 n 维超立方体模映射隐写算法.

2　相关算法

2.1　EMD 算法

Zhang 与 Wang 提出的 EMD 算法[13],可以将一位 $(2n+1)$ 进制的秘密信息嵌入到 n 个载体像素中,其提取函数为

$$f(g_1,g_2,\cdots,g_n)=\left[\sum_{i=1}^{n}(g_i\times i)\right] \bmod (2n+1) \tag{1}$$

式中,$(g_1,g_2,\cdots,g_n)$ 为载体图像的一组像素值,$n=2,3,\cdots$.

该函数描述了在 n 维超立体坐标系中,某点 $(g_1,g_2,\cdots,g_n)$ 及 n 个坐标轴方向上的相邻点的函数值不相同,且正好是 $(2n+1)$ 进制数的数码 $(0,1,2,\cdots,2n)$. 如图 1 所示的 2D 坐标中的函数值分布.

因此,该函数实现最多修改一个像素值为 1,即可嵌入 1 位 $(2n+1)$ 进制秘密信息.

2.2　FEMD 算法

文献[20]提出的全方位 EMD 算法(FEMD),可以实现将一位 a^2 进制的秘密信息嵌入到两个载体像素中,其信息提取函数为

$$f(x,y)=[(a-1)\times x+a\times y] \bmod a^2 \tag{2}$$

式中,(x,y) 为载体图像的一对像素值,$a=2,3,\cdots$.

该函数的特点是,在 2D 坐标系,(x,y) 像素对在由式(2)在像素值[0,255]范围内生成的 256×256 像素对映射矩阵中,其边距离 (x,y) 点为 $r=\lfloor a/2\rfloor$ 的正方形区域内所有元素(函数值)等于或包含 a^2 进制数的数码 $(0,1,2,\cdots,a^2-1)$,如图 2(a)和(b)所示.

因此,该算法的信息嵌入过程就是在该 256×256 矩阵中,在其边距离 (x,y) 点为 r 的正方形内的元素所组成的矩阵中,查找元素等于要嵌入的 a^2 进制信息 d,且 (x,y) 像素对修改量最小的修改方案.

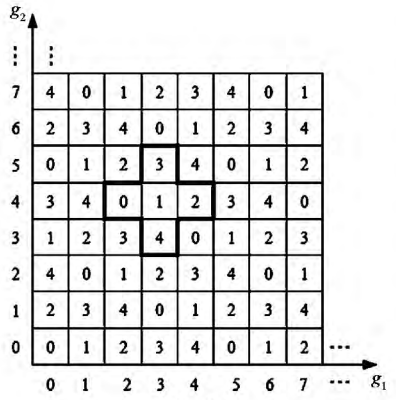
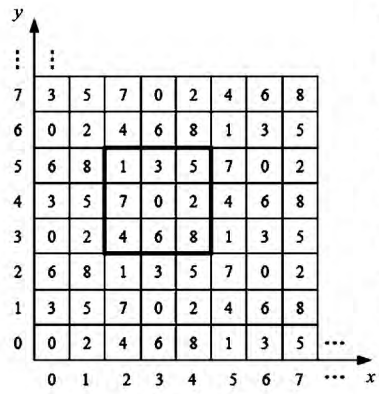
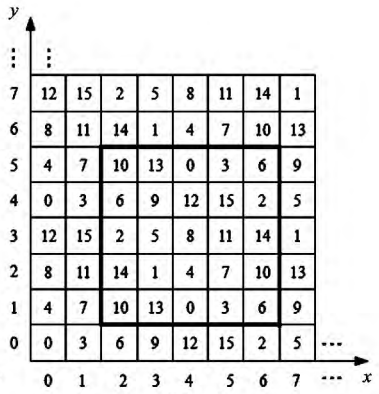


图1　2D矩阵映射，n=2



(a) n=3



(b) n=4

图2　像素对映射矩阵

3　n 维超立方体模映射隐写算法

3.1　模运算性质

模运算函数表示为

$$f=x \bmod a;\quad a=2,3,\cdots \tag{3}$$

对于式(3)所表示的模运算函数,具有以下性质:

性质 1　当 a 为奇数,x 的变化量 Δx 在由式(4)所确定的 a 个连续不同的整数集合 A 内取值时,式(5)成立. 函数 $f(x)$ 是“一对一”的映射关系.

性质 2　当 a 为偶数,x 的变化量 Δx 在由式(4)所确定的 $a+1$ 个连续不同的整数集合 A 内取值时,式(5)成立,且 $f(x+a/2)=f(x-a/2)$. 函数 $f(x)$ 是“多对一”的映射关系.

$$A=\{\Delta x\in Z\mid -\lfloor a/2\rfloor\leqslant\Delta x\leqslant\lfloor a/2\rfloor\} \tag{4}$$

$$\{f\mid f=(x+\Delta x) \bmod a\}=\{0,1,2,\cdots,a-1\} \tag{5}$$

因此,应用模运算这一正负间周期的特点,可以在像素值修改量 Δx 最小的情况下,通过修改像素值 x 为 $x+\Delta x$ 来隐藏一位 a 进制信息 d ($d=0,1,2,\cdots,a-1$). 当 $a=2^k$ 时,可以通过修改像素值 x 为 $x+\Delta x$ 来隐藏 k 位二进制信息. 将式(3)的载体像素 x 扩展至 n 个像素,将得到 n 维超立方体模映射隐写算法.

3.2　n 维超立方体模映射隐写算法

n 维超立方体模映射隐写算法可以实现将一位 a^n 进制秘密信息嵌入到 n 个载体像素中.

3.2.1　相关定义、定理

定义 1　n 维超立方体模映射(n-Dimensional Hy-

percube Modulo Mapping,nDHMM) 信息隐藏(简称 n 维模映射,nDMM),是指将 n 个像素值通过线性组合后的模运算结果映射到一位 a^n 进制秘密信息,从而实现信息隐藏.

设一位 a^n 进制秘密信息嵌入到 n 个其像素值为 $x_1,x_2,\cdots,x_n$ 的载体像素中,算法的提取函数定义为

$$f(x_1,x_2,\cdots,x_n)=\left(\sum_{i=1}^{n}a^{i-1}x_i+c\right)\bmod a^n \tag{6}$$

式中,$a=2,3,\cdots$; $n=1,2,3,\cdots$; c 为引入的算法安全系数,是 x_i 的线性函数值平移量,根据模运算的余数循环的周期性,$c=0,1,2,3,\cdots,a^n-1$.

定理 1 式(6)中,当 x_i 的变化量 Δx_i 都在由式(4)所确定的整数集合 A 内取 a 个连续不同的变化量时,式(7)成立,即在 a^n 个像素值组合的 n 维超立方体编码中的元素正好是 a^n 进制数的数码$(0,1,2,\cdots,a^n-1)$.

$$\{f\mid f=[\sum_{i=1}^{n}a^{i-1}(x_i+\Delta x_i)+c]\bmod a^n\}=\{0,1,2,\cdots,a^n-1\} \tag{7}$$

证明 略.

推理 1 式(6)中,当 a 为偶数,x_i 的变化量 Δx_i 都在由式(4)所确定的集合 A 内取值($a+1$ 个变化量)时,式(7)成立,即在$(a+1)^n$个像素值组合的模映射中的元素包含 a^n 进制数的数码$(0,1,2,\cdots,a^n-1)$,有$(a+1)^n-a^n$个 f 值重复.

由定理 1 和推理 1 可知,在 n 维超立方体坐标系中,某一点$(x_1,x_2,\cdots,x_n)$的 $\pm\lfloor a/2\rfloor$ 的超立方体空间范围内的所有点的函数值 f 一定等于(当 a 为奇数时)或包含(当 a 为偶数时) a^n 进制数的数码$(0,1,2,\cdots,a^n-1)$. 因此可以实现 a^n 进制信息隐藏. 信息嵌入就是遍历这些点的函数值 f 等于 a^n 进制信息 d 的点(当 a 为奇数时),且离$(x_1,x_2,\cdots,x_n)$最近的点(当 a 为偶数时).

当 $a=2^k$ 时,本算法具有 LSBs 一样的嵌入率 k.

3.2.2 嵌入过程

根据前面的叙述,信息隐藏嵌入步骤如下:

(1) 二进制信息流转 a^n 进制信息流

依次取二进制数据流 D 的 L 位数字,将其转化为 K 位 a^n 进制的数字序列. L、K 的取值计算式为

$$L=\lfloor K\log_2 a^n\rfloor \tag{8}$$

当 $a=2^k$ 时,可以用一位 a^n 进制信息完全表示 nk 位二进制信息,即 $K=1$,$L=nk$.

(2) 取 1 位 a^n 进制信息 d,由密钥产生的随机序列选择 n 个载体像素的像素值 x_i 作为一组$(x_1,x_2,\cdots,x_n)$,并按式(6)计算其函数值 f. 如果 $f=d$,不改变像素 x_i,否则按下面规则确定像素 x_i 的修改量:

当 $a=2k+1$,即奇数时,Δx_i 按式(4)所确定的集合 A,通过遍历 Δx_i,使

$$f(x_1+\Delta x_1,x_2+\Delta x_2,\cdots,x_n+\Delta x_n)=d \tag{9}$$

当 $a=2k$,即偶数时,Δx_i 按式(4)所确定的集合 A,通过遍历 Δx_i,在 $f(x_1+\Delta x_1,x_2+\Delta x_2,\cdots,x_n+\Delta x_n)=d$ 下,取总像素值修改量平方(即方差)总和最小时的 Δx_i 的修改方案,即像素值修改满足

$$\begin{cases}f(x_1+\Delta x_1,x_2+\Delta x_2,\cdots,x_n+\Delta x_n)=d\\ \min(\Delta x_1^2+\Delta x_2^2+\cdots+\Delta x_n^2)=true\end{cases} \tag{10}$$

则载密像素值 $x_i'=x_i+\Delta x_i,\ i=1,2,\cdots,n$ (11)

(3) 如计算载密像素 x'_i 溢出,即 $x'_i<0$,或 $x'_i>255$ 时,则分别按式(12)调整,然后再重新嵌入信息.

$$\begin{cases}x_i=x_i+1 & (x_i'<0)\\ x_i=x_i-1 & (x_i'>255)\end{cases} \tag{12}$$

反复执行 2-3,直至信息嵌入完毕.

例 1 $a=3$,$n=2$,$c=1$,$x_1=52$,$x_2=63$,a^n 进制信息 $d_1=5$.

a 奇数,嵌入过程与计算结果如表 1 所示.

由表中的计算结果,函数值 $f=d_1$ 的修改量为

$\Delta x_1=0$,$\Delta x_2=-1$,

$x'_1=x_1+\Delta x_1=52$,$x'_2=x_2+\Delta x_2=62$.

表 1 像素值变化量与函数值

步骤	Δx_1	Δx_2	$f(x_1+\Delta x_1,x_2+\Delta x_2)$
1	0	0	8
2	-1	-1	4
3	-1	0	7
4	-1	+1	1
5	0	-1	5

例 2 $a=2$,$n=2$,$c=0$,$x_1=52$,$x_2=63$,a^n 进制信息 $d_2=3$.

a 偶数,嵌入过程与计算结果如表 2 所示.

表 2 像素值变化量与函数值

步骤	Δx_1	Δx_2	$f(x_1+\Delta x_1,x_2+\Delta x_2)$
1	0	0	2
2	-1	-1	3
3	-1	0	1
4	-1	+1	3
5	0	-1	0
6	0	+1	0
7	+1	-1	1
8	+1	0	3
9	+1	+1	1

由表中的计算结果,$f=d_2$ 的最小修改量为

$\Delta x_1=+1$,$\Delta x_2=0$,

$x'_1=x_1+\Delta x_1=53$,$x'_2=x_2+\Delta x_2=63$.

3.2.3 提取过程

从载密图像提取二进制秘密信息的步骤:

(1) 由密钥产生的随机序列从载密图像选择 n 个

像素为一组$(x'_1,x'_2,\cdots,x'_n)$,从中提取的一位 a^n 进制秘密信息为 $d=f(x'_1,x'_2,\cdots,x'_n)$.

(2) 将提取的 a^n 进制信息转二进制信息.

反复执行 1 -2,直至信息提取完毕.

当不知 K 和 L 的取值时将得不到正确的信息数制转换,在一定程度上提高了算法的安全性.

例 3　从例 1 的载密像素中提取的秘密信息为

$$d_1=f(x'_1,x'_2)=(52+3\times62+1)\bmod 9=5=101\text{B}$$

从例 2 的载密像素中提取的秘密信息为

$$d_2=f(x'_1,x'_2)=(53+2\times63)\bmod 4=3=11\text{B}.$$

3.2.4　嵌入率

本文算法的嵌入率为

$$Payload=\log_2 a \tag{13}$$

3.2.5　载密图像失真度理论分析

载密图像视觉质量通常用峰值信噪比 PSNR 评价,256 级灰度图像的 PSNR 定义为

$$\text{PSNR}=10\times\log_{10}(255^2/\text{MSE}) \tag{14}$$

式中,Mean Squared Error(MSE)为原图像与载密图像之间的均方差,计算式为

$$\text{MSE}=\frac{1}{m\times n}\sum_{i=1}^{m}\sum_{j=1}^{n}(x_{i,j}-x'_{i,j})^2 \tag{15}$$

式中,m 和 n 分别为图像的高和宽,$x_{i,j}$和 $x'_{i,j}$分别为原图像和载密图像(i,j) 像素的像素值.

PSNR 越大,其图像质量越高. 一般要求 PSNR > 30dB,理想的图像视觉质量要求 PSNR > 39dB.

为从理论上比较 LSBs,OPAP,LSBMR,EMD,FEMD 和本文算法的载密图像视觉质量,下面计算这些算法的均方差 MSE. 设秘密信息数据在{0,1}或 $[0,2n]$ 或 $[0,a^n-1]$ 范围内均匀分布.

对于 LSBs,当嵌入率为 k 时,LSBs 的像素值最大修改量为 2^k-1,每一位被修改为 0 和 1 的可能性一样,低第 i 位的均方差为$(1/2)\times(2^{i-1})^2$. 所以,嵌入 k 位 LSBs 的载密图像的均方差为

$$\text{MSE}_{\text{LSB}}=\frac{1}{2}\sum_{i=1}^{k}(2^{i-1})^2=\frac{1}{6}(4^k-1) \tag{16}$$

对于 OPAP,像素值最大修改量为 2^{k-1}. 设原图像像素值为 x,载密像素值为 x'. $|x-x'|=0$ 或$|x-x'|=2^{k-1}$ 的可能性是 $1/2^k$,$|x-x'|$在 $[1,2^{k-1}-1]$ 内的可能性是 $1/2^{k-1}$. 所以,嵌入 k 位信息的 OPAP 的均方差为

$$\text{MSE}_{\text{OPAP}}=\frac{1}{2^k}(2^{k-1})^2+\frac{1}{2^{k-1}}\sum_{i=1}^{2^{k-1}-1}i^2=\frac{1}{12}(4^k+2) \tag{17}$$

对于 EMD,n 个像素中的任一像素被改变 1 的可能性是 $2n/(2n+1)$. 所以,该算法的均方差为

$$\text{MSE}_{\text{EMD}}=\frac{1}{n}\times\frac{2n}{2n+1}=\frac{2}{2n+1} \tag{18}$$

对于 LSBMR,最多只改变两个像素中的一像素值为 1,且被改变 1 的可能性是 3/4. 所以,该算法的均方差为 $\text{MSE}_{\text{LSBMR}}=0.375$.

对于 FEMD 算法,信息嵌入方案是像素值改变最小的方案,可以用式(19)计算其均方差.

$$\begin{aligned}\text{MSE}_{\text{FEMD}}&=\frac{1}{2a^2}\sum_{i=0}^{a^2-1}((x-x_i)^2+(y-y_i)^2)\\&=\frac{1}{2a^2}\sum_{i=0}^{a^2-1}(\Delta x_i^2+\Delta y_i^2)\end{aligned} \tag{19}$$

对于本文算法,信息嵌入方案是像素值方差和改变最小的方案,其均方差为

$$\begin{aligned}\text{MSE}_{n\text{DMM}}&=\frac{1}{na^n}\sum_{i=0}^{a^n-1}((x_1-x_{1i})^2+(x_2-x_{2i})^2+\cdots)\\&=\frac{1}{na^n}\sum_{i=0}^{a^n-1}(\Delta x_{1i}^2+\Delta x_{2i}^2+\cdots+\Delta x_{ni}^2)\end{aligned} \tag{20}$$

根据以上典型算法和本文算法的均方差 MSE 和峰值信噪比 PSNR 的理论分析计算式,将这些算法的 PSNR 比较数据列表如表 3 所示.

表 3 数据表明,本文算法 1DMM 的 PSNR 与 OPAP 相同,但算法比 OPAP 简单、可选嵌入率多得多; 1DMM 的 PSNR 远大于 LSBs; 当 $a=2$ 时,本文算法 2DMM 的 PSNR 与 LSBMR 一样,但 LSBMR 只有一种嵌入率 1bpp.

当 $a=2$ 时,本文算法的 PSNR 大于 EMD.

对于 FEMD 和本文算法,当 a 为奇数时,对于任一信息只有一种像素值修改方案,PSNR 相同; 由推理 1 知,当 a 为偶数时,对某些信息可提供多种像素值修改方案,可以取得更小的像素值修改量. 表 3 的理论计算数据表明,当 $a=2$,本文算法 4DMM 的载密图像质量明显优于 FEMD,PSNR 比 FEMD 高出 0.1848dB; 当 $n>2$,$a>2$,且 a 为偶数时,本文算法的载密图像质量优于 FEMD.

4　实验结果与分析

已通过大量实验证明本文算法的有效性和可行性,限于篇幅,在此仅给出代表性的实验结果. 本次实验采用 Matlab2012b 平台,实验图像选用大小都是 512×512 的 Lena,Airplane,Peppers 和 Baboon 的标准灰度图像,如图 3 所示; a^n 进制秘密信息是由 Lorenz 混沌序列处理得到的随机 a^n 进制信息,信息嵌入像素位置由 Lorenz 混沌序列随机确定,随机选择安全系数 c 的有序随机整数序列也由 Lorenz 混沌序列处理得到. 为使实验简便有效,安全系数 c 按每次嵌入操作在 $[0,a^n-1]$ 内随机选择.

表3 本文算法与 LSBs,OPAP,LSBMR,EMD,FEMD 的 PSNR 比较

a	嵌入率(bpp)	平均峰值信噪比 PSNR(dB)								
		LSBs	OPAP	LSBMR	EMD	FEMD	本文算法			
							1DMM	2DMM	3DMM	4DMM
2	1	51.1411	51.1411	52.3905	52.1102	52.3905	51.1411	52.3905	52.3905	52.5753
3	1.59	—	—	—	—	49.8917	49.8917	49.8917	49.8917	49.8917
4	2	44.1514	46.3699	—	—	46.7478	46.3699	46.7478	46.8141	46.8603
5	2.32	—	—	—	—	45.1205	45.1205	45.1205	45.1205	45.1205
6	2.59	—	—	—	—	43.2997	43.1248	43.2997	43.3395	43.3621
7	2.81	—	—	—	—	42.1102	42.1102	42.1102	42.1102	42.1102
8	3	37.9189	40.7272	—	—	40.8270	40.7272	40.8270	40.8523	40.8659
9	3.17	—	—	—	—	39.8917	39.8917	39.8917	39.8917	39.8917
10	3.32	—	—	—	—	38.9010	38.8366	38.9010	38.9183	38.9273
11	3.46	—	—	—	—	38.1308	38.1308	38.1308	38.1308	38.1308
12	3.59	—	—	—	—	37.3239	37.2791	37.3239	37.3365	37.3429
13	3.7	—	—	—	—	36.6695	36.6695	36.6695	36.6695	36.6695
14	3.81	—		—	—	35.9890	35.9560	35.9890	35.9985	36.0033
15	3.91	—	—	—	—	35.4201	35.4201	35.4201	35.4201	35.4201
16	4	31.8469	34.8064	—	—	34.8317	34.8064	34.8317	34.8392	34.8429

4.1 本文算法实验

本实验,a^n 进制随机信息嵌满载体图像的所有像素;从载密图像提取的 a^n 进制随机信息与嵌入时的 a^n 进制随机信息完全一致.

(a) Lena (b) Airplane (c) Peppers (d) Baboon

图3 载体图像

n 维超立方体模映射隐写算法在不同模 a^n 下的嵌入率和载密图像视觉质量的实验结果如表 4 所示. 由表 4 中的实验数据表明,算法可以提供精细大范围的嵌入率选择,且载密图像可以达到比较好的图像质量,当 a 为偶数且 n 较大时,可获得更好的视觉质量;不同类型图像的实验结果非常一致,也与表 3 的理论分析计算结果很一致,这就证明了本文算法适合不同类型的载体图像,以及本文算法的载密图像均方差分析是正确的.

随着 n 的增加,可以减少嵌入操作次数,但时间复杂度却以 a^n 增长. 一般建议采用 2DMM 和 4DMM,如嵌入率小或采用并行算法,则可采用 8DMM. 采用 8DMM 算法,嵌入率为 1bpp 时,像素均方差 MSE 为 0.3472,PSNR 可达 52.7254dB.

当嵌入率 $Payload$ = 3bpp 时,PSNR 大于理想值 39dB. 当嵌入率 $Payload$ = 4 bpp 时,PSNR 近似 35dB,一维模映射隐写算法 1DMM 各实验载密图像的视觉质量如图 4 所示. 与图 3 的原图像相比,无任何失真现象,仍

(a) Lena (b) Airplane (c) Peppers (d) Baboon

图4 1DMM载密图像*Payload*=4 bpp

保持良好的图像视觉质量.

4.2 与 EMD 等典型算法比较实验

本次实验在载体图像(Lena)、秘密信息、嵌入位置等同等实验条件下进行各种算法的实验仿真比较. EMD 算法在 $n=2$ 时取得算法的最大理论嵌入率为 1.16bpp,本实验用 2 位五进制信息表示 4 位二进制信息,即实际嵌入率为 1bpp. 本次实验项目安排及实验结果如表 5 所示. 表 5 的实验结果表明,与表 3 的理论分析计算结果一致,由此证明这些算法的载密图像均方差分析是正确的.

表 4　不同 a^n 值的嵌入率和图像质量

a	嵌入率(bpp)	峰值信噪比 PSNR(dB)							
		1DMM: $(x+c) \bmod a$				2DMM: $(x_1+ax_2+c) \bmod a^2$			
		Lena	Airplane	Peppers	Baboon	Lena	Airplane	Peppers	Baboon
2	1	51.1401	51.1426	51.1401	51.1168	52.3893	52.4039	52.3938	52.3987
3	1.59	49.8907	49.8985	49.8916	49.8875	49.8907	49.8938	49.8787	49.8921
4	2	46.3839	46.3699	46.3650	46.3731	46.7534	46.7482	46.7419	46.7348
5	2.32	45.1100	45.1262	45.1289	45.1300	45.1268	45.1180	45.1254	45.1149
6	2.59	43.1225	43.1165	43.1371	43.1210	43.2855	43.2924	43.2914	43.3064
7	2.81	42.1088	42.1217	42.1039	42.1079	42.1283	42.1057	42.1145	42.1282
8	3	40.7214	40.7147	40.7238	40.7263	40.8465	40.8263	40.8254	40.8227
9	3.17	39.8796	39.8988	39.8848	39.8964	39.9004	39.8987	39.9064	39.8859
10	3.32	38.8318	38.8373	38.8272	38.8217	38.9140	38.8999	38.8965	38.8995
11	3.46	38.1262	38.1303	38.1160	38.1273	38.1268	38.1293	38.1132	38.1299
12	3.59	37.2781	37.2776	37.2608	37.2731	37.3260	37.3331	37.3253	37.3286
13	3.7	36.6568	36.6667	36.6510	36.6667	36.6798	36.6557	36.6697	36.6704
14	3.81	35.9588	35.9561	35.9603	35.9558	35.9912	35.9890	35.9849	35.9860
15	3.91	35.4200	35.4344	35.4260	35.4354	35.4194	35.4307	35.4151	35.4155
16	4	34.8005	34.8124	34.8143	34.8112	34.8251	34.8360	34.8291	34.8422

续表 4

a	嵌入率(bpp)	峰值信噪比 PSNR(dB)							
		3DMM: $(x_1+ax_2+a^2x_3+c) \bmod a^3$				4DMM: $(x_1+ax_2+a^2x_3+a^3x_4+c) \bmod a^4$			
		Lena	Airplane	Peppers	Baboon	Lena	Airplane	Peppers	Baboon
2	1	52.3814	52.3900	52.3898	52.3959	52.5739	52.5722	52.5797	52.5735
3	1.59	49.8977	49.8956	49.8916	49.8835	49.8947	49.8975	49.8921	49.8938
4	2	46.7920	46.7703	46.3656	46.7693	46.8122	46.8159	46.8231	46.8151
5	2.32	45.1208	45.1091	45.1334	45.1241	45.1223	45.1110	45.1241	45.1259
6	2.59	43.3157	43.3289	43.1371	43.3236	43.3467	43.3345	43.3530	43.3446
7	2.81	42.1002	42.1128	42.1024	42.1121	42.1192	42.1187	42.1050	42.1066
8	3	40.8629	40.8496	40.8560	40.8337	40.8446	40.8541	40.8614	40.8518
9	3.17	39.8816	39.8784	39.8738	39.8894	39.8899	39.8767	39.8902	39.8893
10	3.32	38.9068	38.9110	38.8979	38.9079	38.9222	38.9162	38.9205	38.9131
11	3.46	38.1433	38.1259	38.1316	38.1336	38.1363	38.1280	38.1338	38.1298
12	3.59	37.3402	37.3281	37.3438	37.3506	37.3336	37.3419	37.3421	37.3377
13	3.7	36.6716	36.6716	36.6642	36.6758	36.6720	36.6677	36.6629	36.6716
14	3.81	35.9965	36.0015	35.9890	35.9952	36.0042	35.9952	36.0072	35.9901
15	3.91	35.4074	35.4183	35.4228	35.4091	35.4311	35.4294	35.4056	35.4186
16	4	34.8333	34.8367	34.8348	34.8332	34.8339	34.8450	34.8474	34.8340

表 5 典型算法和本文算法的实验项目及实验结果

a	嵌入率(bpp)	峰值信噪比 PSNR(dB)								
		LSBs	OPAPLSBs	LSBMR	EMD	FEMD	本文算法			
							1DMM	2DMM	3DMM	4DMM
2	1	51.1249	51.1374	52.3825	52.1097	52.3893	51.1401	52.3893	52.3814	52.5739
3	1.59	—	—	—	—	49.8927	49.8907	49.8907	49.8977	49.8947
4	2	44.1433	46.3648	—	—	46.7625	46.3839	46.7534	46.7920	46.8122
5	2.32	—	—	—	—	45.1204	45.1100	45.1268	45.1208	45.1223
6	2.59	—	—	—	—	43.2989	43.1225	43.2855	43.3157	43.3467
7	2.81	—	—	—	—	42.1049	42.1088	42.1283	42.1002	42.1192
8	3	37.9193	40.7357	—	—	40.8467	40.7214	40.8465	40.8629	40.8446
9	3.17	—	—	—	—	39.8938	39.8796	39.9004	39.8816	39.8899
10	3.32	—	—	—	—	38.9001	38.8318	38.9140	38.9068	38.9222
11	3.46	—	—	—	—	38.1200	38.1262	38.1268	38.1433	38.1363
12	3.59	—	—	—	—	37.3223	37.2781	37.3260	37.3402	37.3336
13	3.7	—	—	—	—	36.6600	36.6568	36.6798	36.6716	36.6720
14	3.81	—	—	—	—	35.9978	35.9588	35.9912	35.9965	36.0042
15	3.91	—	—	—	—	35.4162	35.4200	35.4194	35.4074	35.4311
16	4	31.7906	34.8058	—	—	34.8255	34.8005	34.8251	34.8333	34.8339

5 结束语

理论分析与实验结果表明,本文提出的 nDMM 算法与众多的隐写算法相比,具有如下重要特点:

(1) nDMM 算法增加或提高了参数取值的密钥空间,可以更有效抵御隐写分析和非法提取秘密信息.

(2) nDMM 算法完全可以替代 LSB、LSBs、LSBM 和 LSBMR 等基于 LSB 的隐写算法,以及这些算法在其它隐写算法中的应用[10~12],并大幅度提高这些隐写算法的"失真-嵌入量(PSNR,嵌入率)"性能和安全性.

(3) nDMM 算法与 EMD 及基于 EMD 的隐写算法相比,"失真-嵌入量"性能更进一步接近理论值,更好的安全性;当 $a=2^k$ 时,避免了信息数制转换中的数据冗余问题;具有更好的应用灵活性与方便性,可以象基于 LSB 的算法的应用[10~12]和文献[22]的隐写方案一样,灵活方便地结合像素差、像素边缘匹配和图像局部复杂度等自适应隐写算法思想研究新的高性能自适应隐写算法;特别适合基于块的自适应隐写算法的应用,这不仅提高嵌入效率,而且提高载密图像视觉质量.

(4) 选择大的参数 n 且 a 为偶数时,可以得到更好的载密图像视觉质量.

(5) 根据瞿治国博士等人[18]和张新鹏教授等人[19]的研究成果,以及基于 LSB 的算法在频域中的应用[7~9,13],nDMM 算法同样适合 DCT 和 DWT 频域信息隐藏和其他媒体的信息隐藏.

参考文献

[1] Bender W, Gruhl D, Morimoto N, et al. Techniques for data hiding [J]. IBM System Journal, 1996, 35(3-4): 313-336.

[2] Fridrich J, Goljan M, Du R. Detecting LSB steganography in color and grayscale images [J]. IEEE Multimedia, 2001, 8(4): 22-28.

[3] Sharp T. An implementation of key-based digital signal steganography [A]. Proceedings of 4th International Workshop on Information Hiding [C]. Springer LNCS, 2001. 2137: 13-26.

[4] 罗向阳,陆佩忠,刘粉林. 一类可抵御 SPA 分析的动态补偿 LSB 信息隐藏方法 [J]. 计算机学报, 2007, 30(3): 463-473.
Luo Xiang-yang, Lu Pei-zhong, Liu Fen-lin. A dynamic compensation LSB steganography method defeating SPA [J]. Chinese Journal of Computers, 2007, 30(3): 463-473. (in Chinese)

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

[6] Chan C K, Cheng L M. Hiding data in images by simple LSB substitution [J]. Pattern Recognition, 2004, 37(3): 469-474.

[7] Jessica J Fridrich, Miroslav Goljan, David Soukal. Searching for the stego-key [A]. Security, Steganography, and Watermarking of Multimedia Contents VI [C]. USA, 2004. 5306: 70-82.

[8] 刘劲,康志伟,何怡刚. 一种基于小波对比度和 LSB 的密写 [J]. 电子学报, 2007, 35(7): 1391-1393.
LIU Jin, KANG Zhi-wei, HE Yi-gang. A steganographic method based on wavelet contrast and LSB [J]. Acta Electronica Sinica, 2007, 35(7): 1391-1393. (in Chinese)

[9] 陶然,张涛,李文祥,等. 应用整数小波变换的抗盲检测图像隐写 [J]. 应用科学学报,2010,28(6):592 - 600.
TAO Ran,ZHANG Tao,LI Wen-xiang,et al. Images steganography against blind detection using integer wavelet transform [J]. Journal of Applied Sciences,2010,28(6):592 - 600. (in Chinese)

[10] Yang C H,Weng C Y,Wang S J. Adaptive data hiding in edge areas of images with spatial LSB domain systems [J]. IEEE Transactions on Information Forensics and Security,2008,3(3):488 - 497.

[11] Luo W Q,Huang F J,Huang J W. Edge adaptive image steganography based on LSB matching revisited [J]. IEEE Transactions on Information Forensics and Security,2010,5(2):201 - 214.

[12] Lou D C,Wu N I,Wang C M,et al. A novel adaptive steganography based on local complexity and human vision sensitivity [J]. The Journal of Systems and Software,2010,83:1236 - 1248.

[13] Zhang X P,Wang S Z. Efficient steganographic embedding by exploiting modification direction [J]. IEEE Communications Letters,2006,10(11):781 - 783.

[14] Lee C F,Wang Y R,Chang C C. A steganographic method with high embedding capacity by improving exploiting modification direction [A]. Third International Conference on Inter-national Information Hiding and Multimedia Signal Processing [C]. IEEE,2007. 497 - 500.

[15] Kuo W C,Wuu L C,Shyi C N,et al. A data hiding scheme with high embedding capacity based on general improving exploiting modification direction method [A]. Ninth International Conference on Hybrid Intelligent Systems [C]. IEEE,2009. 69 - 72.

[16] Chao R M,Wu H C,Lee C C,et al. A novel image data hiding scheme with diamond encoding [J]. EURASIP Journal on Information Security,2009(2009):658047. 1 - 9.

[17] 廖琪男. 利用模运算及其周期性特点的安全隐写算法 [J]. 中国图象图形学报,2012,17(10):1206 - 1212.
LIAO Qi-nan. Secure steganography based on modulo and its cyclical characteristic [J]. Journal of Image and Graphics,2012,17(10):1206 - 1212. (in Chinese)

[18] Qu Z G,Fu Y,Niu X X,et al. Improved EMD steganography with great embedding rate and high embedding efficiency [A]. Proceedings of Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing [C]. IEEE,2009. 348 - 352.

[19] 张新鹏,刘焕,张颖春,等. 融合方向编码和湿纸编码的高效信息隐藏 [J]. 上海大学学报(自然科学版),2010,16(1):1 - 4.
ZHANG Xin-peng,LIU Huan,ZHANG Ying-chun,et al. Efficient data embedding by combining modification direction modulation and wet paper code [J]. Journal of Shanghai University (Natural Science),2010,16(1):1 - 4. (in Chinese)

[20] Kieu T D,Chang C C. A steganographic scheme by fully exploiting modification directions [J]. Expert Systems with Applications,2011,38(8):10648 - 10657.

[21] Wang X T,Chang C C,Lin C C,et al. A novel multi-group exploiting modification direction method based on switch map [J]. Signal Processing,2012(92):1525 - 1535.

[22] 廖琪男. 基于边缘匹配和模函数的安全密写算法 [J]. 电子学报,2012,40(10):2002 - 2008.
LIAO Qi-nan. Secure steganographic algorithm based on side match and modular function [J]. Acta Electronica Sinica,2012,40(10):2002 - 2008. (in Chinese)

作者简介

廖琪男　男,1964 年 4 月出生,广西钟山人,教授,主要研究方向为数字图像处理、数字图像加密、信息隐藏.
E-mail: lqner@163.com