

改进的基于模函数的数据隐藏方案

刘开会, 徐江峰

(郑州大学 信息工程学院, 郑州 450001)

(luckykaihui2009@sina.com)

摘要: Lee 等人(LEE C F, CHEN H L. A novel data hiding scheme based on modulus function. The Journal of Systems and Software, 2010, 83(5): 832-843)提出了一种基于模函数的数据隐写方法,在图像质量可接受的情况下,每个像素的最大嵌入容量为4位二进制数。但是当每个像素的嵌入量为4位时,隐写图像的质量较差,容易引起攻击者的注意。对该方法进行了改进,缩小了像素改变的范围。理论分析及模拟实验表明,改进方法不但保留了原方法的各种优点,而且使PSNR值增加1.5~3.5 dB,提高了隐写图像的视觉不可见性及抵御RS攻击的能力。

关键词: 隐写方法;模函数;峰值信噪比;RS攻击

中图分类号: TP391.41; TP309 **文献标志码:** A

Improved data hiding scheme based on modulus function

LIU Kai-hui, XU Jiang-feng

(School of Information Engineering, Zhengzhou University, Zhengzhou Henan 450001, China)

Abstract: The new method proposed by Lee et al. (LEE C F, CHEN H L. A novel data hiding scheme based on modulus function. The Journal of Systems and Software, 2010, 83(5): 832-843) was based on modulus function. In this method, each pixel can carry a maximum of 4 bits with an acceptable visual quality. When each pixel is embedded with 4 bits, the quality of stego-images is much worse; as a result, this may catch the attention of attackers. Consequently, this paper improved the method, which narrowed the range that pixels changed. The theoretical analysis and simulation results show that the new method not only keeps the various advantages of original method, but also makes the Peak Signal-to-Noise Ratio (PSNR) value increase 1.5~3.5 dB. Thus, it can raise imperceptibility and the ability resisting RS attack of stego-images.

Key words: steganographic method; modulus function; Peak Signal-to-Noise Ratio (PSNR); RS (Regular Singular) attack

0 引言

数据隐藏是一种伪装术,它实现了隐藏于载体中的秘密信息,在约定双方和多方之间进行不可见传输^[1]。隐藏秘密信息的载体有多种,如:图像、文本、音频等。隐藏方法一般分为数字水印和隐写术。这两者的应用目的不同,数字水印主要用于认证和版权保护,侧重于含密图像的鲁棒性和安全性;而隐写术的主要应用是秘密通信,侧重于嵌入容量和视觉不可见性^[2]。

隐写术的目的是在发送方和接收方之间建立一个隐蔽的通信,潜在的攻击者不知道通信的存在,从而隐藏了信息本身的存在。在隐写方法中,最简单和被众人所知的是最低有效位(Least Significant Bit, LSB)替代法,该方法直接替换载体图像像素的最低 k 位来嵌入信息,能够得到较高的嵌入容量。由于不考虑统计信息的变化等,该方法得到的图像质量并不高而且容易受RS攻击^[2]。2003年Chan等人又提出了基于LSB的OPAP(Optimal Pixel Adjustment Process)方法^[3],该方法首先进行LSB替代,然后对像素进行一系列调整,在保持相同嵌入量的同时,提高了隐写图像质量。2006年Mielikainen提出了一种LSB匹配法^[4],根据载体像素的最低位与秘密数据相同与否进行嵌入,得到的图像质量较好,但是每个像素只能隐藏一位。除此之外,国内外学者还提出了多种其他的隐写方法。2003年,Wu等人提出了利用像素差

(Pixel Value Difference, PVD)进行空间域隐藏的方法^[5],它首先计算相邻两个像素的差值,根据差值判断像素对属于平滑区域还是边缘区域,然后针对不同区域进行不同容量的嵌入。该方法不仅能够获得较好的图像质量,而且还能够抵御RS攻击。后来,许多基于PVD的方法相继被提出^[6-7]。此外,2006年Zhang和Wang提出了嵌入方向拓展(Exploiting Modification Direction, EMD)方法^[8],Kim等人在此基础上提出了改进的嵌入方向拓展法^[9]。

2010年Lee等人提出了一种新的基于模函数的数据隐藏方法^[1],该方法嵌入容量大,有一定的安全性,但是还存在一些缺陷,如图像质量不是很好,用RS分析得到的实验结果也不尽人意。针对其缺陷,本文在此方法的基础上进行了改进。实验证明,改进的方法在保持原有优点的同时,进一步提高了视觉不可见性和安全性。

1 基于模函数的数据隐藏方法

一个 $M \times N$ 的载体图像 I ,像素记为 x ;伪装图像 I' ,像素记为 x' 。在嵌入数据之前,用两个函数 $H_r(R_1, \alpha)$, $H_c(R_2, \beta)$ 选择两个集合 $Kr = \{Kr_i | i = 1, 2, \dots, 2^\alpha\}$, $Kc = \{Kc_j | j = 1, 2, \dots, 2^\beta\}$,其中 $R_1 \in [1, 2^\alpha!]$, $R_2 \in [1, 2^\beta!]$ 。 $\alpha + \beta$ 是每个像素需要隐藏的二进制位数。 Kr 中的每个元素值互不相同,而且其十进制数值在 $[0, 2^\alpha - 1]$ 内。同样, Kc 中的每个元素 Kc_j 也不相同,其十进制落在 $[0, 2^\beta - 1]$ 范围内。在该方法中,

收稿日期:2010-12-31;修回日期:2011-02-24。

作者简介:刘开会(1986-),女,山东德州人,硕士研究生,主要研究方向:信息隐藏;徐江峰(1965-),男,河南禹州人,教授,博士,主要研究方向:信息安全、混沌加密通信。

R_1, R_2, α, β 是四个密钥。秘密数据比特流记为 S 。把 S 分成许多段 S_k, S_k 又分为 S_{k1} 和 S_{k2} , 即 $S_k = S_{k1} \parallel S_{k2}$, 其中 S_{k1} 包含 α 位数据, S_{k2} 包含 β 位数据。 α 和 β 越大, 则嵌入容量越大。例1说明了根据函数 $H_r()$ 和 $H_c()$ 如何得到集合 Kr 和 Kc 。

例1 假设 $\alpha = 3, \beta = 2, R_1 = 2, R_2 = 24, 0 \sim 2^\alpha - 1$ 共 2^α 个数据组成的全排列如表1所示, $0 \sim 2^\beta - 1$ 共 2^β 个数据组成的全排列如表2所示。根据 $H_r(R_1, \alpha) = H_r(2, 3)$, $H_c(R_2, \beta) = H_c(24, 2)$, 得到 $Kr = \{000, 111, 100, 011, 010, 101, 110, 001\}$, $Kc = \{11, 01, 00, 10\}$ 。

表1 $0 \sim 2^\alpha - 1$ 的所有排列方式

R_1	排列
1	{001, 010, 000, 100, 011, 111, 110, 101}
2	{000, 111, 100, 011, 010, 101, 110, 001}
\vdots	\vdots
40320	{111, 100, 010, 011, 001, 110, 101, 000}

表2 $0 \sim 2^\beta - 1$ 的所有排列方式

R_2	排列
1	{10, 00, 11, 01}
2	{00, 11, 10, 01}
\vdots	\vdots
24	{11, 01, 00, 10}

Kr 和 Kc 集合产生后, 它们的值可以进一步形成变异笛卡尔积 $Kr \otimes Kc$, 不同于笛卡尔积, 变异笛卡尔积 $Kr \otimes Kc$ 由 Kr 和 Kc 产生一个有 $2^\alpha \times 2^\beta$ 个元素的有序集合, 集合中的元素不是有序对, 而是一个二进制串。即

$$Kr \otimes Kc = \{Kr_i \parallel Kc_j \mid Kr_i \in Kr, Kc_j \in Kc, i = 1, 2, \dots, 2^\alpha, j = 1, 2, \dots, 2^\beta\} \quad (1)$$

其中: $Kr_i \parallel Kc_j$ 表示 Kr_i 与 Kc_j 连接后得到的长度为 $\alpha + \beta$ 的二进制串, 并且其十进制数值在 $[0, 2^{\alpha+\beta} - 1]$ 内。根据 $Kr_i \parallel Kc_j$ 位串, 可以计算出其位置 $d (d \in [1, 2^{\alpha+\beta}])$ 。

$$d = 2^\beta \times (i - 1) + j \quad (2)$$

其中: i, j 分别为 S_{k1}, S_{k2} 在 Kr, Kc 中的位置; d 是一个十进制数, 表示 S_k 的位置。

集合 G 表示用来隐藏数据的像素 x 可变换的像素集, 它由模函数

$$f(x) = x \bmod n \quad (3)$$

和像素 x 产生。假设 $\gamma = f(x)$, 则 $G = \{g_i \mid i = 1, 2, \dots, n\} = \{x - \gamma, x - \gamma + 1, \dots, x - \gamma + n - 1\}$, 其中, $n = 2^{\alpha+\beta}$ 。例2描述了如何产生像素集。

例2 $\alpha = 2, \beta = 2, x_1 = 16, x_2 = 79$ 。根据式(3)可得, $\gamma_1 = 16 \bmod 2^4 = 0, \gamma_2 = 79 \bmod 2^4 = 15, G_1 = \{16 - 0, 16 - 0 + 1, 16 - 0 + 2, \dots, 16 - 0 + 14, 16 - 0 + 15\}, G_2 = \{79 - 15, 79 - 15 + 1, 79 - 15 + 2, \dots, 79 - 15 + 14, 79 - 15 + 15\}$, 如图1所示, 方格内的数据表示像素值, 方格下方的数据表示对应像素的位置。

16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

(a) x_1 的像素集 G_1

64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

(b) x_2 的像素集 G_2

图1 原方法产生的像素集

像素集产生后, 根据式(2)计算 $\alpha + \beta$ 位秘密数据在

$Kr \otimes Kc$ 中的位置 d , 则 G 中的第 d 个元素即是伪装像素值 x' , 即 $x' = g_d$ 。这样就完成了数据的嵌入。在秘密数据提取过程中, 授权方用已知密钥 α, β, R_1, R_2 , 获得 Kr 和 Kc 集合, 然后用式(1)生成变异笛卡尔积。根据隐秘图像的像素值 x' 计算 $d, d = x' \bmod n + 1$, 然后从 $Kr \otimes Kc$ 中得到第 d 个元素 S_k , 则 S_k 即为秘密数据。

该方法与传统的 LSB 替代法相比, 安全性有所提高, 但是进行隐写后的图像质量与 LSB 替代法基本相同。当每个像素隐藏 n 位时, 对于载体像素 x , 其像素的最大改变量仍然为 $2^n - 1$; 当 n 较大时, 隐写图像的质量较差。为此, 本文对此方法进行了改进, 以减小像素的最大改变量。

2 改进后的方法

改进后的方法仍然利用模函数进行隐秘数据的嵌入和提取, 区别在于 x 像素集的产生方法不同, 嵌入过程中 x 并不是由像素集中第 d 个元素来代替, 而是由像素集中模为 $d - 1$ 的元素来代替。当每个像素嵌入 1 位时, 与原方法得到的图像质量相同, 当每个载体像素嵌入 n 位时, $n \in \{2, 3, 4\}$, 除了少数像素外, 大多数像素的最大改变量从 $2^n - 1$ 下降到 2^{n-1} 。

2.1 数据嵌入过程

输入: 密钥 α, β, R_1, R_2 , 载体图像 I , 嵌入数据 S 。

输出: 隐写图像 I' 。

- 1) 取 I 的像素值 x , 从 S 中取出 $\alpha + \beta$ 位数据 $S_k, S_k = S_{k1} \parallel S_{k2}, S_{k1}$ 为 α 位, S_{k2} 为 β 位。
- 2) 根据密钥得到两个集合 Kr, Kc 。
- 3) 根据 $S_{k1} = Kr_i, S_{k2} = Kc_j$ 得到 i, j 。
- 4) 根据式(2)计算位置 d 。
- 5) 生成 x 的像素集 G, G 中的元素为连续的 2^k 个数值, 其模值落在 $[0, 2^k - 1]$ 内, 且互不相同。从像素集 G 中查找模为 $d' = d - 1$ 的元素, 此元素即为 x' 。

载体像素 x 的像素集为 $group(x + 1)$, 像素集的生成如下:

$$c = 2^k, k = \alpha + \beta$$

$$\text{① if } x + 1 \in [1, c/2 + 1]$$

$$\text{for } j = 1 : c$$

$$group(x + 1, j) = j - 1$$

$$\text{② if } x + 1 \in [c/2 + 2, 256 - (c/2 - 1)]$$

$$\text{for } j = 1 : c$$

$$group(x + 1, j) = x - c/2 + j - 1$$

$$\text{③ if } x + 1 \in [256 - (c/2 - 2), 256]$$

$$base = 256 - (c/2 - 1)$$

$$\text{for } j = 1 : c$$

$$group(x + 1, j) = group(base, j)$$

- 6) 重复步骤 1) ~ 5) 直到所有数据嵌入完毕。

2.2 数据提取过程

输入: 密钥 α, β, R_1, R_2 , 隐写图像 I' ;

输出: 秘密数据 S 。

- 1) 扫描隐写图像 I' , 得到像素值 x' ;
- 2) 根据 $H_r(R_1, \alpha)$ 和 $H_c(R_2, \beta)$ 分别得到两个集合 Kr, Kc ;
- 3) 利用公式 $d' = x' \bmod n$ 得到模值 d' ;
- 4) 从 $Kr \otimes Kc$ 中取位置为 $d = d' + 1$ 的元素, 此元素即为秘密数据 S_k 。

- 5) 重复步骤 1) ~ 4) 直到所有数据提取完毕。

利用上述方法, 对于给定的条件: $R_1 = 12, R_2 = 9, \alpha = 2, \beta = 2, x_1 = 16$ 与 $x_2 = 79$ 产生的像素集如图2所示, 方格内的数据表示像素, 方格下方的数据表示对应像素的模值。根据

$H_r(12,2)$ 和 $H_c(9,2)$ 得出 $Kr = \{11,01,00,10\}$, $Kc = \{00,11,10,01\}$ 。当嵌入数据为 '0101 1100' 时,原方法得到 $x_1' = 23, x_2' = 64$, 而改进方法得到 $x_1' = 23, x_2' = 80$ 。由此可以看出,改进方法的像素改变值要小于等于原方法的像素改变值。

8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
8	9	10	11	12	13	14	15	0	1	2	3	4	5	6	7

(a) x_1 的像素 G_1

71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86
7	8	9	10	11	12	13	14	15	0	1	2	3	4	5	6

(b) x_2 的像素 G_2

图2 改进方法得出的像素集

提取数据时,改进方法与原方法是相同的。根据 $H_r(12,2)$ 和 $H_c(9,2)$ 得出 $Kr = \{11,01,00,10\}$, $Kc = \{00,11,10,01\}$ 。隐写图像像素值分别为 $x_1' = 23, x_2' = 80$, 计算得到 d' 的值分别为 7、0, 从 $Kr \otimes Kc$ 中查找位置为 $d = d' + 1$ 的元素, 即位置分别为 8、1 的元素, 可得到秘密数据: 0101 1100。

3 实验仿真

考查一个隐藏方案的优劣一般有四个标准,分别为嵌入容量、算法复杂度、视觉不可见性和安全性^[1]。改进方法与原方法相比,在保持相同嵌入量和算法复杂度下,进一步提高了视觉不可见性和安全性。为了分析改进方法的特性,选取多幅图像进行实验,实验工具为 Matlab。下面从视觉不可见性和安全性方面对两种方法进行对比分析。

3.1 视觉不可见性

隐写方法中一般用峰值信噪比 (Peak Signal-to-Noise Ratio, PSNR) 来衡量隐密图像质量的视觉不可见性^[1]。隐密图像的 PSNR 值越高,视觉不可见性越好;反之越差。用原方法与改进方法分别对灰度图像 Baboon. bmp, Lena. bmp, Elaine. bmp 进行数据嵌入,嵌入数据后图像的 PSNR 比较结果如表 3 所示。

$$PSNR = 10 \lg \frac{255^2}{MSE} \quad (4)$$

$$MSE = \frac{1}{M \times N} \sum_{i=1}^M \sum_{j=1}^N (x_{ij} - x'_{ij})^2 \quad (5)$$

其中,255 是 8 位灰度图像像素的最大值,均方误差 (Mean Square Error, MSE) 是计算 $M \times N$ 的载体图像 I 与隐写图像 I' 的平均方差, x_{ij} 和 x'_{ij} 分别表示 I 与 I' 的像素值。

表3 原方法与改进方法得到的 PSNR 值的对比

载体图像 (512 × 512)	每个像素 嵌入位数	文献[1] 的 PSNR/dB	改进后的 PSNR/dB
Baboon	1	49.629	49.629
	2	42.431	44.853
	3	36.730	39.245
	4	30.216	33.568
Lena	1	50.824	50.824
	2	43.683	46.080
	3	37.885	40.431
	4	31.383	34.544
Elain	1	50.712	50.712
	2	43.500	45.946
	3	37.887	40.381
	4	31.466	34.563

以 Lena. bmp 为载体图像嵌入数据,每个像素嵌入 4 位二进制数据,原方法和改进方法得出的图像如图 3 所示。从图中可以看出原方法得到的隐写图像质量较差,而用改进方法

嵌入相同数据后的图像质量有明显改善,不容易引起攻击者的注意。

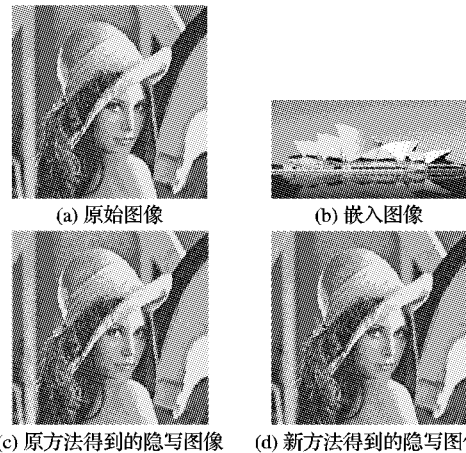


图3 两种方法隐写图像对比

3.2 安全性

RS (Regular Singular) 检测方法是 Jessica Fridrich 等人提出的一种隐写分析法^[10],具有较高的可靠性和灵敏度。RS 分析首先将待检测图像分为很多大小相等的图像块,再对每个小图像块进行 F_1 操作 (F_1 为 $2i$ 与 $2i+1$ 之间的互翻转操作),然后利用式 (6) 计算其混乱度是否增加,并计算混乱度增加的图像块和混乱度减小的块在所有图像块中所占比例,分别记为 R_m, S_m ; 然后应用 F_{-1} 操作 (F_{-1} 为 $2i-1$ 与 $2i$ 之间的互翻转操作),在每个图像块中进行类似的处理,也记下混乱度增加和减小的图像块在所有图像块中所占比例,分别为 R_{-m}, S_{-m} 。如果待检测图像没有经过隐写,那么无论应用 F_1 操作还是 F_{-1} 操作,从统计特性上来说,会同等地增加图像块的混乱度,即 $R_m \approx R_{-m}, S_m \approx S_{-m}$, 且 $R_m > S_m, R_{-m} > S_{-m}$ 。

$$f(X) = \sum |X - X_1| + \sum |X - X_2| \quad (6)$$

其中, X 是图像块的灰度值矩阵, X_1 表示将 X 左移一列, X_2 表示将 X 下移一行, $f(X)$ 表示相邻像素灰度差值的绝对值总和。用 RS 分析法分别对文献[1]中的方法和改进后的方法进行分析,如图 4、5 所示。

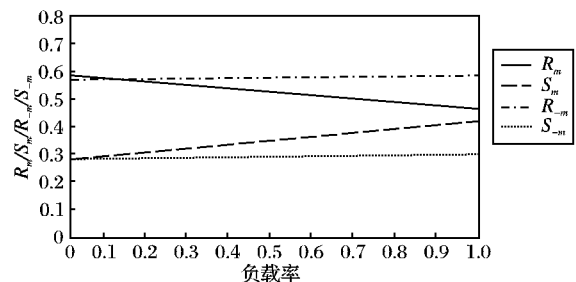


图4 RS 分析法对文献[1]方法的实验结果

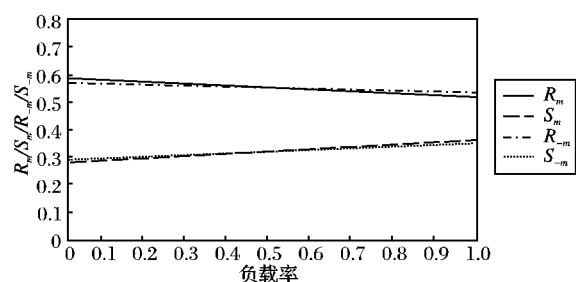


图5 RS 分析法对改进方法的实验结果

从图 4 与图 5 可以看出,原方法得出的 R_m 与 R_{-m}, S_m 与 S_{-m} (下转第 1975 页)

- demodulator with 3-to-5GHz agile synthesizer for 9-band WiMedia UWB in 65nm CMOS [C]// Proceedings of the IEEE International Solid-State Circuits Conference. Washington, DC: IEEE, 2009: 412–413.
- [18] LIU H Y, LIN C C, LIN Y W, *et al.* A 480Mb/s LDPC-COFDM-based UWB baseband transceiver [C]// Proceedings of the IEEE International Solid-State Circuits Conference. Washington, DC: IEEE, 2005: 444–445, 609.
- [19] Wisair 531 integrated MAC\baseband UWB chip, pre-production 2nd generation UWB WiMedia\MBOA-compliant chip [EB/OL]. [2010-08-22]. <http://www.wisair.com/wp-content/Wisair531.pdf>.
- [20] LEENAERTS D, BEEK R, BERGERVOET J, *et al.* A 65 nm CMOS inductorless triple band group WiMedia UWB PHY [J]. IEEE Journal of Solid-State Circuits, 2009, 44(12): 3499–3510.
- [21] FONTANA R J. Recent system applications of short-pulse ultra-wideband (UWB) technology [J]. IEEE Transactions on Microwave Theory and Techniques, 2004, 52(9): 2087–2104.
- [22] WANG X, QIN B, XIE H L, *et al.* FCC-EIRP-aware UWB pulse generator design approach [C] // Proceedings of the IEEE International Conference on Ultra-Wideband. Washington, DC: IEEE, 2009: 592–596.
- [23] MCCORKLE J. Ultra wide bandwidth (UWB): Gigabit wireless communications for battery operated consumer applications [C]// Proceedings of the IEEE Symposium on VLSI Circuits. Washington, DC: IEEE, 2005: 6–9.
- [24] GENG C H, PEI Y K, GE N. An iterative multipath interference-canceller with linear equalization for ultra high data rate DS-UWB system [C]// Proceedings of the IEEE International Conference on Ultra-Wideband. Washington, DC: IEEE, 2009: 93–97.
- [25] CHEN Y, ZHANG J, JAYALATH A D S. Multiband OFDM UWB vs IEEE802.11n: system level design considerations [C]// Proceedings of the IEEE Vehicular Technology Conference. Washington, DC: IEEE, 2006: 1972–1976.
- [26] SABERINIA E, TEWFIK A H. Single and multi-carrier UWB communications [C]// Proceedings of the International Symposium on Signal Processing and Its Applications. Washington, DC: IEEE, 2003: 343–346.
- [27] EMAMI S, CORRAL C, RASOR G. Peak-to-average power ratio (PAPR), fractional bandwidth and processing gain of UWB schemes [C]// Proceedings of the IEEE International Symposium on Spread Spectrum Techniques and Applications. Washington, DC: IEEE, 2004: 929–933.
- [28] TROESCH F, STEINER C, ZASOWSKI T, *et al.* Hardware aware optimization of an ultra low power UWB communication system [C]// Proceedings of the IEEE International Conference on Ultra-Wideband. Washington, DC: IEEE, 2007: 174–179.
- [29] CAPOGLU I R, LI Y, SWAMI A. Effect of Doppler spread in OFDM-based UWB systems [J]. IEEE Transactions on Wireless Communications, 2005, 4(5): 2559–2567.
- [30] YAK C W, LEI Z D, CHATTONG S, *et al.* Timing synchronization and frequency offset estimation for ultra-wideband (UWB) multi-band OFDM systems [C]// Proceedings of the IEEE International Symposium on Personal, Indoor and Mobile Radio Communications. Washington, DC: IEEE, 2005: 471–475.
- [31] LAI H Q, SIRI WONGPAIRAT W P, LIU K J R. Performance analysis of multiband OFDM UWB systems with imperfect synchronization and intersymbol interference [J]. IEEE Journal of Selected Topics in Signal Processing, 2007, 1(3): 521–534.
- [32] MIRI R, ZHOU L, HEYDARI P. Timing synchronization in impulse-radio UWB: trends and challenges [C]// Proceedings of the Joint 6th International IEEE Northeast Workshop on Circuits and Systems and TAISA Conference. Washington, DC: IEEE, 2008: 221–224.
- [33] HE N, TEPEDELENLIOGLU C. Performance analysis of non-coherent UWB receivers at different synchronization levels [J]. IEEE Transactions on Wireless Communications, 2006, 5(6): 1266–1273.

(上接第1919页)

S_m 的差值相差很大,而改进后的 R_m 与 R_{-m} , S_m 与 S_{-m} 的差值相差比较小,因此安全性有所提高。

4 结语

本文对文献[1]所提出的方法进行了改进,数据嵌入方法不同,数据提取方法是相同的。如果每个像素嵌入 n ($n \in \{2, 3, 4\}$) 位数据,对于8位的灰度图像,原方法中对于所有 $pixel \in [0, 255]$ 的像素,其改变范围为 $[0, 2^n - 1]$; 而改进的方法对于 $pixel \in [0, 2^{n-1} - 2] \cup [255 - (2^{n-1} - 2), 255]$ 的像素,改变范围为 $[0, 2^n - 1]$, 其余像素与原方法相同,改变范围为 $[0, 2^{n-1}]$ 。实验证明,改进后的方法在保持相同嵌入量的同时,隐秘图像的视觉不可见性和安全性都有所提高。

参考文献:

- [1] LEE C F, CHEN H L. A novel data hiding scheme based on modulus function [J]. The Journal of Systems and Software, 2010, 83(5): 832–843.
- [2] 许欢, 王建军. 利用分块像素差和模函数的大容量信息隐藏方法 [J]. 信息与电子工程, 2009, 7(3): 218–221.
- [3] CHAN C K, CHENG L M. Hiding data in images by simple LSB substitution [J]. Pattern Recognition, 2004, 37(3): 469–474.
- [4] MIELIKAINEN J. LSB matching revisited [J]. IEEE Signal Processing Letters, 2006, 13(5): 285–287.
- [5] WU D C, TSAI W H. A steganographic method for images by pixel-value differencing [J]. Pattern Recognition Letters, 2003, 24(9/10): 1613–1626.
- [6] WU H C, WU N I, TSAI C S, *et al.* Image steganographic scheme based on pixel-value differencing and LSB replacement methods [J]. IEE Proceeding—Vision Image and Signal Processing, 2005, 152(7): 611–615.
- [7] WANG C M, WU N I, TSAI C S, *et al.* A high quality steganographic method with pixel-value differencing and modulus function [J]. Journal of Systems and Software, 2008, 81(1): 150–158.
- [8] ZHANG X P, WANG S Z. Efficient steganographic embedding by exploiting modification direction [J]. IEEE Communication Letters, 2006, 10(11): 781–783.
- [9] KIM H J, KIM C, CHOI Y, *et al.* Improved modification direction methods [J]. Computers and Mathematics with Application, 2010, 60(2): 319–325.
- [10] FRIDRICH J, GOLJAN M, DU R. Detecting LSB steganography in color and gray-scale images [J]. Magazine of IEEE Multimedia: Special Issue on Security, 2001, 8(4): 22–28.