像素差自适应隐写方案 *

潘 峰[1a,1b,2], 刘 圆[1a], 王世峰[3]

(1. 武警工程学院 a. 网络与信息安全武警部队重点实验室; b. 信息安全研究所, 西安 710086; 2. 西安电子科技大学 网络信息安全教育部重点实验室, 西安 710071; 3. 武警山东省总队, 济南 251010)

摘 要: 提出了一种新的基于相邻像素差的自适应隐写算法。该算法结合图像位平面性质以及人眼对像素值起伏剧烈的区域敏感性较差的视觉特性,根据相邻像素高五位比特值之差的不同选择不同的嵌入策略,通过改变每对像素的最低三位比特值实现信息嵌入。通过理论分析和实验证明,该算法具有较高的嵌入容量,具有良好的隐写安全性,同时算法复杂度低,实现简单。

关键词: 视觉特性; 空域隐写算法; 像素差; 高安全性

中图分类号: TP391 **文献标志码**: A **文章编号**: 1001-3695(2012)02-0655-03

doi:10.3969/j.issn.1001-3695.2012.02.067

Adaptive steganographic algorithm on pixel-value differencing

PAN Feng[1a,1b,2], LIU Yuan[1a], WANG Shi-feng[3]

(1. *a. Key Laboratory of Network & Information Security, b. Institute of Information Security, Engineering College of Armed Police Force, Xi' an* 710086, *China*; 2. *Key Laboratory of Network & Information Security of Ministry of Education, Xidian University, Xi' an* 710071, *China*; 3. *Shandong Supreme Bureau of Chinese Armed Police Force, Jinan* 251010, *China*)

Abstract: This paper proposed a new adaptive steganographic algorithm based on pixel-value differences between adjacent pixels. The algorithm realized embedding messages by combing the nature of image bit-planes with the human vision quality that eyes were not sensitive to the area where pixels changed frequently and acutely. It chose different embedding strategies according to the differences between the first five bit planes of two adjacent pixels, and modified the last three bit planes of them. Through the theoretical analysis and the experiment results, it proves that the algorithm can obtain high capacity and obtain strong steganography security. Besides, the algorithm has low complexity and can be easily realized.

Key words: vision quality; steganography in space domain; pixel-value differencing; high security

0 引言

20 世纪 90 年代以来,信息隐藏技术在网络安全中的作用日益凸显,数字图像隐写术成为了信息隐藏领域的一大研究热点。

图像隐写技术分为空域隐写算法和变换域隐写算法。由于具有更高嵌入容量、更好的视觉质量等优点,相比变换域算法,空域隐写算法应用更加广泛。最原始的空域隐写算法最低有效位(least significant bit, LSB)替代[1]及其扩展 JSteg[1]、LHA[2]和 MLSB[3]都得到广泛应用。Kawaguchi 等人提出的位平面复杂度分割(bit-plane complexity segmentation, BPCS)密写[1]和 Wu 等人[4]提出的 PVD(pixel-value differencing)密写是最常见的利用人类视觉特性和图像复杂度的隐写算法,该算法由于 R_K 的划分使直方图出现了阶梯现象。Zhang 等人提出的改进的 PVD 算法通过动态划分 R_K,更好地消除了原始 PVD 算法中存在的阶梯效应[5]。2005 年 Wu 等人[6]提出了基于 PVD 和 LSB 的图像隐写方案,该算法融合了 PVD 算法和 LSB 算法,再次提高了算法的安全性与嵌入量。2006 年,Yang 等人[7]提出了多像素差的数字图像隐写方法,根据含四个像素的小块的三个像素差进行自适应嵌入,有效地提高了 PVD 的嵌入效率。2006 年,Zhang 等人[8]提出了嵌入方向拓展(exploiting modification direction, EMD),其在 n 个图像载体中最多只需改动一个载体数据便可隐藏一个 $2n+1$ 进制的秘密信息,充分利用不同嵌入方向实现高效数据隐藏。2009 年,Jung 等人[9]利用模运算提出了改进的 EMD 算法,提高了 EMD 算法的嵌入率。2010 年,Yang 等人在文献[10]中综述了各种融合 PVD 和 LSB 的空域算法,并通过低像素差的调整策略提出了新的改进算法,有效地提高了算法安全性。

本文利用人眼对像素值起伏剧烈区域敏感性较差的视觉特性[4],提出了一种新的相邻像素差自适应隐写算法,根据相邻像素二进制取值的高位差的不同选择不同的嵌入方法。理论分析与性能对比表明,新方法可保证较好的视觉不可见性和统计不可见性。

1 信息隐藏算法及提取原理

1.1 信息嵌入介绍

将秘密消息隐藏在图像两个相邻像素的灰度值中。图像的主要信息大多存在高位平面上,通过计算相邻像素二进制值

收稿日期: 2011-07-09; **修回日期**: 2011-08-18 **基金项目**: 国家自然科学基金资助项目(60842006);武警工程学院基础基金资助项目(wjy201027)

作者简介:潘峰(1967-),男,陕西西安人,副教授,博士,主要研究方向为信息安全、多媒体处理;刘圆(1986-),女,硕士,主要研究方向为信息隐藏(198605311coo@163.com);王世峰(1984-),男,硕士,主要研究方向为信息研究.

的高五位的差值,差值大则表明此处像素值波动较大,可选择修改率较大的嵌入方法;差值小则表明此处像素值波动较小,可选择修改率较小的嵌入方法。在相同的嵌入条件下与经典的 LSB 及其改进相比,本算法在确保视觉不可见性和统计不可见性的前提下,有效地提高了嵌入率。

1.2　信息嵌入过程

从载体图像中顺序提取两相邻像素。提取的方法有很多,如逐行、逐列或 zigzag 扫描,本文使用逐行扫描。记图像中逐行扫描像素点得到的一维向量为 $f_1,f_2,f_3,\cdots,f_n$,将欲嵌入的二进制秘密比特序列与伪随机序列作模 2 和,得到待嵌比特序列。算法如下:

a)取相邻两像素 f_i 和 $f_{i+1}(1\leqslant i<n)$,令

$$f_i=(x_1x_2x_3x_4x_5x_6x_7x_8)_2$$

$$f_{i+1}(y_1y_2y_3y_4y_5y_6y_7y_8)_2$$

其中,下角标 2 表示二进制序列,下同。

b)判断像素值高五位的差值,根据差值选择嵌入算法。若 $|(x_1x_2x_3x_4x_5)_2-(y_1y_2y_3y_4y_5)_2|\leqslant 1$,则进行如下操作(其中加减运算均为数值运算):

(a)预先从待嵌比特中顺序取出三位比特位记为 $(s_1s_2s_3)_2$,

若 $s=4$,则取三比特秘密信息 $(s_1s_2s_3)_2$;

若 $s\neq 4$,则取二比特秘密信息 $(s_1s_2)_2$;

(b)令 $x_{6'}=0,y_{6'}=0$;令 $k=[(x_{6'}x_7x_8)_2\times 1+(y_{6'}y_7y_8)_2\times 2-S]\bmod 5$,

当 $k=0$ 时,转至(d);

当 $k=1$ 时,令 $(y_{7'}y_{8'})_2=(y_7y_8)_2$;

若 $(x_7x_8)_2\neq 0$,则 $(x_{7'}x_{8'})_2=(x_7x_8)_2-1$;

若 $(x_7x_8)_2=0$,则 $x_{6'}=1$;

当 $k=2$ 时,令 $(x_{7'}x_{8'})_2=(x_7x_8)_2$

若 $(y_7y_8)_2\neq 0$,则 $(y_{7'}y_{8'})_2=(y_7y_8)_2-1$;

若 $(y_7y_8)_2=0$,则 $y_{6'}=1$;

当 $k=3$ 时,令 $(x_{7'}x_{8'})_2=(x_7x_8)_2$;$(y_{6'}y_{7'}y_{8'})_2=(0y_7y_8)_2+1$;

当 $k=4$ 时,令 $(y_{7'}y_{8'})_2=(y_7y_8)_2$;$(x_{6'}x_{7'}x_{8'})_2=(0x_7x_8)_2+1$;

(c)$f_i(x_1x_2x_3x_4x_5x_{6'}x_{7'}x_{8'})_2$,$f_{i+1}=(y_1y_2y_3y_4y_5y_{6'}y_{7'}y_{8'})_2$;

(d)若 $i\leqslant n-3$,则 $i=i+2$,返回步骤 a);否则嵌入过程完成。

若 $|(x_1x_2x_3x_4x_5)_2-(y_1y_2y_3y_4y_5)_2|>1$,则进行如下操作:

(a)从待嵌比特中顺序取出 2 位比特位记为 $(s_1s_2)_2$;

(b)$x_{6'}=\arg\min(|f_i-(x_1x_2x_3x_4x_5x_{6'}s_1s_2)_2|)$,$\arg\min(f(x))$ 表示使 $f(x)$ 取最小值时 x 的值,$f_i(x_1x_2x_3x_4x_5x_{6'}s_1s_2)_2$;

(c)若 $i\leqslant n-2$,则 $i=i+1$,返回步骤 a);否则嵌入过程完成。

1.3　信息提取过程

a)取相邻两像素 f_i 和 $f_{i+1}(1\leqslant i<n)$,令 $f_i=(x_1x_2x_3x_4x_5x_6x_7x_8)_2$,$f_{i+1}=(y_1y_2y_3y_4y_5y_6y_7y_8)_2$。

b)判断像素值高五位的差值,根据差值选择提取算法。

若 $|(x_1x_2x_3x_4x_5)_2-(y_1y_2y_3y_4y_5)_2|\leqslant 1$,则计算 $s=[(x_6x_7x_8)_2\times 1+(y_6y_7y_8)_2\times 2]\bmod 5$;

若 $s=4$,则恢复 3 比特秘密信息 $(s_1s_2s_3)_2$;

若 $s\neq 4$,则恢复 2 比特秘密信息 $(s_1s_2)_2$;

若 $|(x_1x_2x_3x_4x_5)_2-(y_1y_2y_3y_4y_5)_2|>1$,则进行如下操作:

(a)令 $(s_{1'}s_{2'})_2=(x_7x_8)_2$;

(b)若 $i\leqslant n-2$,则 $i=i+1$,返回步骤 a);若 $i>n-2$,跳至步骤 c)。

c)按顺序将提取的比特序列恢复,并与预先的伪随机序列作模 2 和,得到秘密信息。

2　性能分析与比较

通过计算相邻像素二进制取值的高五位的差值,根据差值选择不同的算法,差值大的像素对选用嵌入率高的 2-LSB 算法[3],差值小的像素对选用嵌入效率高的改进的 EMD 算法,在保证嵌入容量的同时有效地提高了算法的视觉不可见性和统计不可见性。

2.1　性能分析

大多数有效的检测算法都是仅针对某一特定的隐写算法,将多种隐写算法合理地融合在一种算法中不失为一种好的方法。EMD 算法能够抵抗针对 LSB 的检测算法,因此结合图像复杂度融合 LSB 与 EMD 算法不仅能提高算法的嵌入容量,同时能抵抗基于 LSB 的检测算法,提高了算法安全性。

根据上文介绍,当差值满足 $|(x_1x_2x_3x_4x_5)_2-(y_1y_2y_3y_4y_5)_2|\leqslant 1$ 时,两像素点的差值范围是[0,15],此时选用 EMD 算法;当差值满足 $|(x_1x_2x_3x_4x_5)_2-(y_1y_2y_3y_4y_5)_2|>1$ 时,两像素点的差值范围是[9,255],此时选用改进的 2-LSB 算法。由于用于判断像素值高五位与用于嵌入秘密消息的像素值低三位相互独立,因此,上述两种情况没有重叠。以大小为 256×256 的 Lena、girl、couple 为例,统计可得像素差的分布情况如表 1 所示。

表 1　示例图像像素差分布

图像		像素差	
		$\|(x_1x_2x_3x_4x_5)_2-(y_1y_2y_3y_4y_5)_2|\leqslant 1$	$\|(x_1x_2x_3x_4x_5)_2-(y_1y_2y_3y_4y_5)_2|>1$
Lena	数值	12 723	20 045
	百分比/%	38.83	61.17
girl	数值	29 056	3 721
	百分比/%	88.67	11.33
couple	数值	28 640	4 128
	百分比/%	87.40	12.60

2.2　性能比较

不可见性是图像隐写术中一个重要指标,人眼不能有效察觉的峰值信噪比(PSNR)为 38 dB[1]。表 2 列出了原始 PVD、改进的 PVD、2-LSB 算法和本文算法的 PSNR 值,本文 PSNR 值远高于 38 dB,优于表中其他算法。图 1、3、5 为 256×256 的原始图像,图 2、4、6 为相应的嵌入秘密后的图像,从图中可以看出,嵌入秘密信息后的图像满足视觉不可见性。

表 3 为 RS 分析[1]所得的嵌入率估计值,表中分别列出了 LSB 满嵌、LSB 嵌入率为 0.7、LSB 嵌入率为 0.3、本文满嵌以及

原始图像的 RS 分析估计值,安全阈值为 0.1 时本文算法能够很好地抵抗 RS 分析,较 LSB 算法有很大的优势,满足统计不可见性。

表 2　嵌入随机比特流后的 PSNR 值

图像	PSNR			
	PVD	改进的 PVD[7]	2-LSB	本方案
Lena	47.787 3	49.263 5	47.945 3	50.706 4
girl	47.368 7	48.915 6	48.203 0	51.428 6
couple	45.162 8	47.438 7	48.186 3	51.854 9

图1　Lena原始图像

图2　Lena载密图像

图3　girl原始图像

图4　girl载密图像

图5　couple原始图像

图6　couple载密图像

表 3　RS 分析的嵌入率估计值

图像	嵌入率估计值				
	正常图像	嵌入率为 1 的 LSB	嵌入率为 0.7 的 LSB	嵌入率为 0.3 的 LSB	本方案
Lena	-0.291 7	0.995 3	0.677 8	0.168 9	-0.111 7
girl	-0.005 1	0.992 8	0.774 5	0.217 8	0.034 1
couple	-0.036 9	1.006	0.757 8	0.281 7	0.039 6

3　结束语

本算法结合人眼视觉特性,借鉴了 PVD 算法的思想,通过对两个子算法进行一定的改进,在保证嵌入率的前提下,能抵抗RS分析,具有良好的视觉不可见性和统计不可见性。今后的研究重点是在保证不可见性的条件下提高算法嵌入效率和嵌入率。

参考文献:

[1] 王朔中,张新鹏,张开文. 数字密写和密写分析[M]. 北京:清华大学出版社,2005:20-83.

[2] ZHANG Xin-peng, WANG Shuo-zhong, ZHANG Kai-wen. Steganography with least histogram abnormality[C]//Lecture Notes in Computer Science, vol 2776. Berlin: Springer-Verlag, 2003:401-412.

[3] 刘粉林,刘九芬,罗向阳,等. 数字图像隐写分析[M]. 北京:机械工业出版社,2010:58.

[4] WU Da-chun, TSAI W H. A steganographic method for images by pixel-value differencing[J]. Pattern Recognition Letters, 2003, 24(9-10):1613-1626.

[5] ZHANG Xin-peng, WANG Shuo-zhong. Vulnerability of pixel-value differencing steganography to historgram[J]. Pattern Recognition Letters, 2004, 25(3):331-339.

[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 Proceedings Vision, Image and Signal Processing, 2005, 152(5):611-615.

[7] YANG C H, WENG C Y. A steganographic method for digital images by multipixel differencing[C]//Proc of IEEE International Computer Symposium. 2006:831-836.

[8] ZHANG Xin-peng, WANG Shuo-zhong. Efficient steganographic embedding by exploiting modification direction[J]. IEEE Communications Letters, 2006, 10(11):781-783.

[9] JUNG K H, YOO K Y. Improved exploiting modification direction method by modulus operation[J]. International Journal of Signal Processing, Image Processing and Pattern, 2009, 2(1):79-87.

[10] YANG C H, WENG Chi-yao, WANG S J, *et al*. Varied PVD + LSB evading detection programs to spatial domain in data embedding systems[J]. Journal of Systems and Software, 2010, 83(10):1635-1643.

(上接第 654 页)

[6] LeFEVRE K, DeWITT D J, RAMAKRISHNAN R. Incognito: efficient full-domain *k*-anonymity[C]//Proc of ACM SIGMOD International Conference on Management of Data. New York: ACM, 2005:49-60.

[7] LI Jie-xing, TAO Yu-fei, XIAO Xiao-kui. Preservation of proximity privacy in publishing numerical sensitive data[C]//Proc of ACM SIGMOD International Conference on Management of Data. New York: ACM, 2008:437-486.

[8] SAMARATI P. Protecting respondents' identities in microdata release[J]. IEEE Trans on Knowledge and Data Engineering, 2001, 13(6):1010-1027.

[9] ZHANG Qing, KOUDAS N, SRIVASTAVA D, *et al*. Aggregate query answering on anonymized tables[C]//Proc of the 23rd IEEE International Conference on Data Engineering. 2007:116-125.

[10] LeFEVRE K, DeWITT D J, RAMAKRISHNAN R. Workload-aware anonymization[C]//Proc of ACM Knowledge Discovery and Data Mining. 2006:277-286.

[11] LI Ning-hui, LI Tian-cheng, VENKATASUBRAMANIAN S. *t*-closeness: privacy beyond *k*-anonymity and *l*-diversity[C]//Proc of of the 23rd IEEE International Conference on Data Engineering. 2007:106-115.

[12] RUBNER Y, TOMASI C, GUIBAS L J. The earth mover's distance as a metric for image retrieval[J]. International Journal of Computer Vision, 2000, 40(2):99-121.

[13] Le FEVRE K, De WITT D J, RAMAKRISHNAN R. Mondrian multidimensional *k*-anonymity[C]//Proc of the 22nd International Conference on Data Engineering. Washington DC: IEEE Computer Society, 2006:277-286.

[14] WANG Ting, MENG S, BAMBA B, *et al*. A general proximity privacy principle[C]//Proc of IEEE International Conference on Data Engineering. Washington DC: IEEE Computer Society, 2009:1279-1282.

[15] WANG Ting, LIU Ling. XColor: protecting general proximity privacy[C]//Proc of the 26th IEEE International Conference on Data Engineering. 2010:960-963.

[16] XIAO Xiao-kui, TAO Yu-fei. Anatomy: simple and effective privacy preservation[C]//Proc of the 32nd International Conference on Very Large Data Bases. 2006:139-150.