第35卷 第2期 华侨大学学报(自然科学版) Vol. 35 No. 2
2014年3月 Journal of Huaqiao University (Natural Science) Mar. 2014

文章编号:1000-5013(2014)02-0136-06 **doi**:10.11830/ISSN.1000-5013.2014.02.0136

利用整数变换的高效图像可逆信息隐藏方法

邱应强[1,2],冯桂[1],田晖[3]

(1. 华侨大学 信息科学与工程学院,福建 厦门 361021;
2. 福州大学 数字媒体研究院,福建 福州 350002;
3. 华侨大学 计算机科学与技术学院,福建 厦门 361021)

摘要: 针对Alattar算法运算复杂度过高的问题,提出一种基于整数变换的高效图像可逆信息隐藏方法.该方法在数据嵌入和提取过程中,只需要对各宿主向量进行一次整数变换,且所有向量通过整数变换后即可直接判定该向量是否可用于嵌入机密数据,降低了数据嵌入和提取过程中的运算复杂度.实验结果表明:该方法具有较大的数据嵌入容量,较好的隐蔽性和较低运算复杂度,在正确提取嵌入数据后可无失真恢复原图像.

关键词: 整数变换;可逆信息隐藏;复杂度;嵌入容量

中图分类号: TP 309 **文献标志码**: A

可逆信息隐藏是近年来信息隐藏领域的一个重要研究分支.由于其在提取嵌入数据后能完全无失真恢复原宿主信息,可逆信息隐藏技术适合应用在要求较高的军事通信、医学诊断等领域.2003年,Tian[1]提出一种基于相邻两像素点差值扩展的图像可逆隐藏方法.该方法先用整数Haar小波变换得到相邻两像素的均值和差值;然后,对差值扩展并嵌入1比特机密数据;最后,将扩展后的差值和均值通过相应整数逆变换得到嵌入数据后的像素值.Tian算法的提出是在可逆信息隐藏研究上的重大突破,后续出现了许多在此基础上的改进算法,但大多还是基于相邻两像素的差值扩展[2-3].文献[2]将差值扩展技术推广到基于预测差值扩展的可逆隐藏方法上,此后也出现了许多相应的改进算法[4-5].2004年,Alattar[6]从另一个角度对Tian算法进行拓展,采用多像素点组成的向量的差值代替两像素对的差值进行扩展,提高了算法的嵌入容量,但算法复杂度较高.2006年,郭志川等[7-8]对Alattar算法进行改进,在一定程度上降低了算法运算复杂度,但对隐藏质量带来了一定的影响.2007年,谢于民等[9]提出了一种基于线性整数变换算法和排序图像可逆数据隐秘传输方法,该方法可嵌入的数据量较大,同时隐蔽性也较好.2012年,邱应强等[10]针对文献[9]中定义的整数变换算法进行改进,改进后的整数变换算法对图像块引入失真减少为文献[9]方法的一半,在相同嵌入数据量情况下,进一步提高了算法的隐蔽性.由于文献[6-8]方法在数据嵌入和提取过程中各宿主向量至少需要进行两次整数变换,并且要逐步判定分成可扩展向量、可修改向量和不可修改向量3类,运算复杂度较高.因此,本文提出了一种基于整数变换的高效图像可逆信息隐藏新方法.

1 系统概述

图像可逆信息隐藏系统的发送端数据嵌入框,如图1所示.首先,对宿主图像分块;然后,对所有图像块进行整数变换并判定是否可用于嵌入数据,用"0","1"值分别标记不可嵌入图像块、可嵌入图像块,并最终形成二值标记值序列,保留可嵌入图像块整数变换后的结果,不可嵌入图像块不作整数变换处理;提取不可嵌入图像块中的部分像素点最低有效位(least significant bit,LSB),并与标记值序列及经加密后的机密数据组合在一起,经伪随机化处理后得到待嵌入数据;待嵌入数据按一定顺序直接替代可

收稿日期: 2013-05-20

通信作者: 邱应强(1981-),男,讲师,主要从事信息隐藏、图像处理的研究.E-mail:yqqiu@hqu.edu.cn.

基金项目: 国家自然科学基金资助项目(61372107,61302094)

嵌入图像块经整数变换后的部分像素，及未经整数变换的不可嵌入图像块部分像素最低有效位实现数据嵌入，所有图像块重组得到隐藏图像.

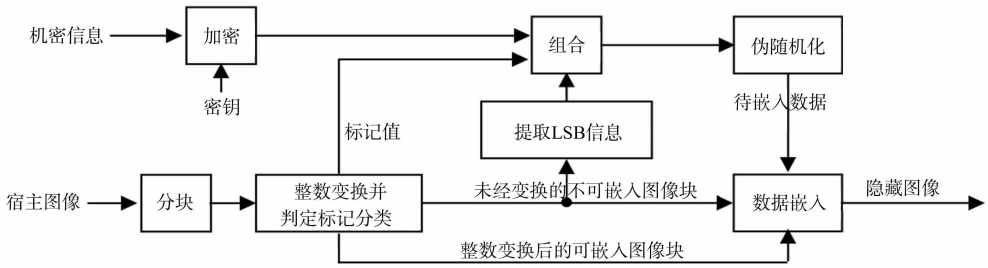

图 1　数据嵌入框图

Fig. 1　Block diagram of data embedding

在提取端，对隐藏图像分块，按特定顺序直接提取所有图像块部分像素点最低有效位得到二值数据序列，经反伪随机化处理得到标记值序列、不可嵌入图像块部分像素的最低有效位序列及加密后的机密数据序列. 最后，对标记值为“0”的图像块用提取的最低有效位序列恢复，而标记值为“1”的图像块则通过整数逆变换无失真恢复.

2　可逆信息隐藏算法

假设图像大小为 $N_1\times N_2$，分成大小为 $n_1\times n_2$ 的互不重叠的图像块，共$\lfloor N_1/n_1\rfloor\times\lfloor N_2/n_2\rfloor$($\lfloor\cdot\rfloor$表示向下取整，下同)个，将图像块 $n=n_1\times n_2$ 个像素点组成向量 $\boldsymbol{v}=(v_1,\cdots,v_i,\cdots,v_n)$，其中 $0\leqslant v_i\leqslant 255$ $(1\leqslant i\leqslant n)$. $\bar{\boldsymbol{v}}$ 定义为

$$\bar{\boldsymbol{v}}=\left\lfloor\frac{\sum_{i=1}^{n}v_i}{n}\right\rfloor. \tag{1}$$

式(1)中：$\sum_{i=1}^{n}v_i$ 不一定能够被 n 整除，计算结果 $\bar{\boldsymbol{v}}$ 将舍去值为 $m/n(m\in 0,1,\cdots,n-1)$ 的小数部分. 因此，有 $n\bar{\boldsymbol{v}}=\sum_{i=1}^{n}v_i-m$.

整数变换定义为

$$v'_i=T_1(v_i)=v_i+(v_i-\bar{\boldsymbol{v}})=2v_i-\bar{\boldsymbol{v}}. \tag{2}$$

组成新向量 $\boldsymbol{v}'=(v'_1,\cdots,v'_i,\cdots,v'_n)$，满足

$$\sum_{i=1}^{n}v'_i=\sum_{i=1}^{n}2v_i-\bar{\boldsymbol{v}}=2\cdot\sum_{i=1}^{n}v_i-\left(\sum_{i=1}^{n}v_i-m\right)=\sum_{i=1}^{n}v_i+m. \tag{3}$$

由于

$$\frac{nv'_i+\sum_{i=1}^{n}v'_i}{2n}=\frac{n(2v_i-\bar{\boldsymbol{v}})+\sum_{i=1}^{n}v_i+m}{2n}=\frac{2nv_i-n\bar{\boldsymbol{v}}+\sum_{i=1}^{n}v_i+m}{2n}=$$

$$v_i+\frac{-\left(\sum_{i=1}^{n}v_i-m\right)+\sum_{i=1}^{n}v_i+m}{2n}=v_i+\frac{m}{n}. \tag{4}$$

式(3)～(4)中：$m\in[0,1,\cdots,n-1]$，有 $0\leqslant m/n<1$. 因此，式(1)对应的整数逆变换为

$$v_i=\left\lfloor\frac{nv'_i+\sum_{i=1}^{n}v'_i}{2n}\right\rfloor. \tag{5}$$

由于图像像素点像素值是介于 0 到 255 之间的整数，因此，图像块向量 $\boldsymbol{v}$ 经过整数变换后得到的向量 $\boldsymbol{v}'=(v'_1,\cdots,v'_i,\cdots,v'_n)$分 2 种情况. 如果 $\boldsymbol{v}'$中的任意元素 v'_i 均在 0 到 255 范围之内，表明可通过整数变换在该图像块中嵌入数据，称为可嵌入图像块，用“1”值标记，归为 S1 类；否则不能通过整数变换在

该图像块中嵌入数据,称为不可嵌入图像块,用"0"值标记,归为S2类.所有图像块标记值可组成$\lfloor N_1/n_1 \rfloor \times \lfloor N_2/n_2 \rfloor$比特二值标记值序列.

根据式(2)整数变换定义,对S1类中的任意可嵌入图像块向量$\boldsymbol{v}'$中的任一元素v_i对应的整数变换式中$2v_i$值均为偶数,再减去相同的平均值取整$\bar{\boldsymbol{v}}$得到新的整数变量v'_i均同为偶数或奇数,即经过整数变换后$\boldsymbol{v}'$中的所有元素最低有效位均为0或1.因此,只需要在$\boldsymbol{v}'$保留第一个元素最低有效位,即可表明$\boldsymbol{v}'$中的所有元素最低有效位是0还是1,其他$n-1$个元素最低有效位均可用待嵌入数据直接替代.对于S2类中的不可嵌入图像块,将不作整数变换,其后$n-1$个像素点像素值最低有效位也用待嵌入数据直接替代,但为了能够无失真恢复不可嵌入图像块,被替代的最低有效位数据需保存作为待嵌入数据的一部分,因此提取不可嵌入图像块中所有被修改的像素最低有效位组成S2_LSB序列.标记值序列、S2_LSB序列和加密后的机密数据序列一起组成二值待嵌入数据序列.嵌入数据时,在保留不可嵌入图像块数据的同时,将所有可嵌入图像块进行整数变换后得到新的图像块信息,再按一定顺序将二值待嵌入数据依次直接替代所有图像块中的后$n-1$个特定像素的最低有效位.

信息提取及图像无失真恢复时,依次提取所有图像块中的后$n-1$个特定像素最低有效位,从中提取出$\lfloor N_1/n_1 \rfloor \times \lfloor N_2/n_2 \rfloor$比特二值标记值序列,根据二值标记序列中"0"值的个数确定不可嵌入图像块的个数,并提取不可修改图像块最低有效位序列,其余二值序列解密得到机密数据.最后,根据二值标记值序列,值为"1"的图像块采用整数逆变换算法无失真恢复,值为"0"的图像块部分像素最低有效位用提取不可修改图像块最低有效位序列依次替代无失真恢复.所有图像块重组得到原宿主图像.

3 数据嵌入或提取步骤

3.1 嵌入步骤

1) 发送端将大小为$N_1 \times N_2$的图像I,分成$n=\lfloor N_1/n_1 \rfloor \times \lfloor N_2/n_2 \rfloor$个大小为$n=n_1 \times n_2$的互不重叠图像块.

2) 对每一图像块组成的n维向量$\boldsymbol{v}$,按照式(2)进行整数变换得到v',判定v'所有元素值是否均在0到255范围内,满足为可嵌入图像块,否则为不可嵌入图像块,分别用"1"值和"0"值进行标记得到标记值序列L,并分别归类至S1类和S2类.S1类图像块数据用整数变换后的图像块数据替代,S2类图像块数据保留不变.提取所有S2类图像块中后$n-1$个像素点的最低有效位,组成二值S2_LSB序列.

3) 标记值序列L、不可嵌入图像块最低有效位序列S2_LSB,以及用密钥Key对机密数据流P加密后,得到数据流P'组成数据流W,再通过伪随机化处理得到待嵌入数据W'.

4) 待嵌入数据W'按特定顺序依次替代所有图像块的后$n-1$个像素点最低有效位,完成数据嵌入.最后所有图像块重组得到隐藏图像I'.

3.2 提取/恢复步骤

1) 接收端将隐藏图像I'分成与发送端相同大小的互不重叠图像块,所有图像块后$n-1$个像素点像素值的最低有效位按特定顺序提取得到嵌入数据W'.

2) 对W'反伪随机化处理得到W,提取W数据流中的标记值序列L,根据L从W数据流中分离出S2_LSB和P'.

3) P'解密后得到机密数据P.

4) 标记值序列L中"1"值对应的图像块采用整数逆变换无失真恢复,"0"值对应的图像块后$n-1$个像素点最低有效位用S2_LSB依次替代无失真恢复.重组所有图像块无失真恢复原宿主图像I.

4 算法复杂度分析

Alattar算法[6]将n个相邻像素点组成图像块向量$\boldsymbol{v}=(v_1,\cdots,v_i,\cdots,v_n)$的整数变换,定义为计算所有向量元素均值,以及$v_2,\cdots,v_n$分别与$v_1$之间的差值.通过对计算得到的$n-1$个差值进行扩展可嵌入$n-1$比特信息,结合扩展后差值和均值可通过逆变换得到嵌入数据后的像素值.算法通过差值扩展后逆变换得到的数值是否在图像像素值范围内,来判定差值是否可扩展用于嵌入数据.由于算法需在嵌

入特定机密数据前对各图像块向量差值扩展性进行判定，判定时对该差值所嵌入的 1 比特机密数据未知，判定向量可扩展性时需要遍历嵌入 2^{n-1} 个可能的 $n-1$ 比特数据组合并且作整数逆变换，判定对应 2^{n-1} 次逆变换后数值是否均在图像像素值范围内，遍历过程中每次需要判定 $2n$ 个不等式，同样不可扩展向量还需要采用类似方法判定向量的可修改性，具有较大的运算复杂度.

Alattar 改进算法[7-8]将整数变换改为计算 n 维像素点向量 $\boldsymbol{v}=(v_1,\cdots,v_i,\cdots,v_n)$ 的所有向量元素均值，以及 $v_1,\cdots,v_n$ 分别与向量中最小像素值减 1 后的差值. 算法改进后只需要判定除其中一个值为 1 的差值外，其余 $n-1$ 个差值均扩展并全部嵌入“1”或全部嵌入“0”后逆变换结果是否均在图像像素值有效范围内，即可判定向量的扩展性. 对于不可扩展向量也通过类似方法进一步判定其可修改性. 算法改进后将 2^{n-1} 次逆变换和变换结果判定减少到 2 次，降低了算法的运算复杂度，但由于扩展差值绝对值变大，会对隐藏图像质量带来一定影响.

式(2)表明，整数变换直接将图像块向量 $\boldsymbol{v}$ 中各元素与向量均值 $\bar{\boldsymbol{v}}$ 之间的差值扩展一倍，从而产生了 $n-1$ 比特冗余信息可用于嵌入数据. 该算法在数据隐藏嵌入和提取过程各图像块向量只需要通过一次整数变换，而且所有向量可对整数变换结果通过 $2n$ 个不等式直接判定分成可嵌入向量和不可嵌入向量两类，进一步降低了算法运算复杂度. 同时扩展差值为各元素与向量均值 $\bar{\boldsymbol{v}}$ 之间的差值，降低了对隐藏图像质量的影响.

5　实验结果分析

为了验证本算法，配备 Intel(R) Core(TM) i5-3210M CPU 的 PC 机进行了仿真实验，实验软件平台为 Visual C^{++} 6.0，宿主图像为大小 512 px×512 px 的 256 级灰度图像 Baboon，F16，Peppers，Man 和 Lena，如图 2 所示，机密数据使用汉字数据. 采用峰值信噪比(R_{SN})衡量隐藏图像质量，R_{SN} 值越高表明隐藏图像质量越好、隐蔽性越好.

Baboon　　F16　　Peppers　　Man　　Lena

图 2　实验宿主图像

Fig. 2　Experimental host images

分别采用 Alattar 算法[6]、Alattar 改进算法[7-8]和文中算法，并分别使用图像块大小参数为 $N=2\times2$ 和 $N=4\times4$，在相同宿主图像中嵌入最大量汉字数据. 采用 Alattar 算法、Alattar 改进算法和文中算法的实验结果，分别如表 1～3 所示. 比较表 1～3 实验数据可知：在最大嵌入容量上 Alattar 改进算法最低、文中算法总体略高于 Alattar 算法；在图像质量上，Alattar 改进算法最低、本文算法与 Alattar 算法基本相当；在嵌入或提取时间上，Alattar 改进算法是本文算法两倍以上，而 Alattar 算法远大于其余两种方法，尤其是在图像块大小增大情况下，嵌入或提取时间随图像块大小近似呈指数式增长.

表 1　Alattar 算法实验结果

Tab. 1　Experimental results of Alattar's algorithm

图像名	$N=2\times2$			$N=4\times4$		
	最大嵌入量/bits	R_{SN}/dB	嵌入或提取时间/ms	最大嵌入量/bits	R_{SN}/dB	嵌入或提取时间/ms
Baboon	129 782	25.07	221.5/116.8	215 456	23.27	250 577.0/127 660.0
F16	129 752	29.68	221.0/118.2	215 411	28.00	251 234.0/127 312.0
Peppers	128 786	33.50	222.4/117.5	213 446	30.50	250 819.0/128 102.0
Man	130 397	30.01	218.1/116.0	219 956	27.38	250 960.0/127 293.0
Lena	130 988	32.73	220.7/119.1	225 641	29.35	254 959.0/127 003.0

表2 Alattar改进算法实验结果

Tab. 2 Experimental Results of Alattar's improved algorithm

图像名	$N=2\times2$			$N=4\times4$		
	最大嵌入量/bits	R_{SN}/dB	嵌入或提取时间/ms	最大嵌入量/bits	R_{SN}/dB	嵌入或提取时间/ms
Baboon	129 713	24.83	20.73/23.62	214 691	23.26	13.77/15.65
F16	129 650	29.42	21.16/23.36	214 991	27.97	13.84/15.60
Peppers	128 528	32.90	21.13/23.17	212 786	30.40	13.63/15.73
Man	130 346	29.65	21.42/23.64	219 581	27.35	13.81/15.66
Lena	130 970	32.23	20.61/23.37	225 596	29.26	13.38/15.52

表3 本文算法实验结果

Tab. 3 Experimental results of the proposed algorithm

图像名	$N=2\times2$			$N=4\times4$		
	最大嵌入量/bits	R_{SN}/dB	嵌入或提取时间/ms	最大嵌入量/bits	R_{SN}/dB	嵌入或提取时间/ms
Baboon	129 785	25.07	8.56/7.03	215 936	23.24	6.91/4.99
F16	129 800	29.66	8.69/7.04	215 621	27.96	6.84/5.05
Peppers	128 831	33.44	8.47/7.03	213 821	30.48	6.96/5.05
Man	130 427	29.99	8.51/7.18	220 166	27.34	6.67/5.11
Lena	130 988	32.73	8.39/6.97	225 671	29.34	6.90/5.24

实验还采用文献[9-10]的算法,使用图像块大小为 $N=2\times2$ 在测试图像中分别嵌入最大量的汉字数据.表4为相应的实验数据,与表3数据对比可以看出:文中算法在嵌入容量、嵌入后图像质量和运算复杂度方面均优于文献[9-10]的算法.

表4 文献[9-10]算法实验结果($N=2\times2$)

Tab. 4 Experimental results of reference [9-10]'s algorithms($N=2\times2$)

图像名	文献[9]算法			文献[10]算法		
	最大嵌入量/bits	R_{SN}/dB	嵌入或提取时间/ms	最大嵌入量/bits	R_{SN}/dB	嵌入或提取时间/ms
Baboon	89 402	20.36	10.87/7.51	94 202	21.46	14.15/10.19
F16	127 354	25.15	11.13/8.81	100 562	27.05	13.65/9.91
Peppers	131 330	25.97	10.93/8.16	100 634	29.62	13.65/10.21
Man	126 546	23.22	11.02/8.15	101 578	26.42	14.15/9.99
Lena	137 698	25.00	10.83/8.19	103 954	28.72	13.83/10.04

隐藏图像通过局域网传输后,接收端均能100%正确地提取嵌入其中的汉字数据,并无失真恢复原图像.

6 结论

给出了一种基于整数变换的高效图像可逆信息隐藏方法.该方法在数据嵌入和提取过程只需要通过一次整数变换,而且所有向量通过整数变换后即可直接判定该向量是否可用于嵌入机密数据,具有较低的运算复杂度.

仿真实验结果表明:该方法在嵌入更大数据量后能保证隐藏图像的质量,并且较大幅度地降低算法数据嵌入和提取时间,具有较好的实时性;同时,在隐藏图像未受到破坏的情况下,可从隐藏图像中正确提取隐藏数据并无失真恢复原宿主图像,具有较高的实用价值.该方法可应用于军事图像、医学图像等质量要求较高的可逆信息隐藏、信息隐秘传输等,也可用于音视频多媒体的可逆信息隐藏.

参考文献:

[1] TIAN Jun. Reversible data embedding using a difference expansion[J]. IEEE Trans Circuits and Systems for Video

Technology,2003,13(8):890-896.

[2] THODI D M,RODRIGUEZ J J. Expansion embedding techniques for reversible watermarking[J]. IEEE Trans Image Processing,2007,16(3):721-730.

[3] HU Yong-jian,LEE H K,CHEN Kai-ying,et al. Difference expansion based reversible data hiding using two embedding directions[J]. IEEE Trans Multimedia,2008,10(8):1500-1512.

[4] LI Xiao-long,YANG Bin,ZENG Tie-yong. Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection[J]. IEEE Trans Image Processing,2011,20(12):3524-3533.

[5] COLTUC D. Low distortion transform for reversible watermarking[J]. IEEE Trans Image Processing,2012,21(1):412-417.

[6] ALATTAR A M. Reversible watermark using the difference expansion of ageneralized integer transform[J]. IEEE Trans Image Processing,2004,13(8):1147-1156.

[7] 郭志川,程义民,王以孝,等. 一种无损的隐秘传输方法与仿真[J]. 系统仿真学报,2006,18(6):1638-1642.

[8] 郭志川,程义民,王以孝,等. 一种基于视频的无损信息隐藏方法[J]. 中国科学院研究生院学报,2006,23(2):165-173.

[9] 谢于明,程义民,田源,等. 基于整数变换的无损隐秘传输方法仿真研究[J]. 系统仿真学报,2007,19(19):4594-4598.

[10] 邱应强,张育钊. 基于改进整数变换的无损隐秘传输方法与仿真[J]. 系统仿真学报,2012,14(6):1096-1101.

Effective Image Reversible Information Hiding Method Based on Integer Transform

QIU Ying-qiang[1,2], FENG Gui[1], TIAN Hui[3]

(1. College of Information Science and Engineering, Huaqiao University, Xiamen 361021, China;
2. Research Academy of Digital Media, Fuzhou University, Fuzhou 360002, China;
3. College of Computer Science and Technology, Huaqiao University, Xiamen 361021, China)

Abstract: According to the high caculation complexity problem of Alattar's agorithm, an effective image reversible information hiding method based on integer transform was proposed. Using the proposed method, every host vector was transformed by integer transform only once during the embedding or extracting process, and after integer transformed, all vectors could be directly determined whether the vector can be used to embed secret information or not, it also reduce the caculation complexity during the embedding and extracting process. The experimental results showed that the method has larger data embedding capacity, better secrecy and lower caculation complexity. After the embedded data was extracted, the original image could be restored without any distortion.

Keywords: integer transform; reversible information hiding; complexity; embedding capacity

（**责任编辑**：黄晓楠　　**英文审校**：吴逢铁）