基于动态失真补偿量化索引调制的可逆数据隐藏算法

叶天语 钮心忻 马兆丰 杨义先
(北京邮电大学网络与交换技术国家重点实验室信息安全中心 北京 100876)
(北京邮电大学网络与信息攻防技术教育部重点实验室 北京 100876)
(北京邮电大学灾备技术国家工程实验室 北京 100876)

摘 要：不同于传统的失真补偿量化索引调制，该文提出了动态失真补偿量化索引调制的概念。两者的区别在于量化步长和失真补偿参数是否可变。首先推导出动态失真补偿量化索引调制可逆性的成立条件，然后推导出失真补偿参数的可允许范围，最后利用可逆性设计一个具体的可逆数据隐藏算法。在只执行一遍时，它的数据隐藏率高达 1 bit 每像素，高于其他可逆数据隐藏算法。另外，算法的动态特性有利于防止参数泄露。实验结果表明：不管初始条件如何，该算法既能正确解码出秘密信息，又能准确恢复原始载体。

关键词：信息隐藏；动态失真补偿量化索引调制；可逆数据隐藏；数据隐藏率
中图分类号：TP391 **文献标识码**： A **文章编号**：1009-5896(2010)06-1489-04
DOI: 10.3724/SP.J.1146.2009.00859

A Reversible Data Hiding Algorithm Based on Dynamic Distortion-Compensated Quantization Index Modulation

Ye Tian-yu Niu Xin-xin Ma Zhao-feng Yang Yi-xian
(*Information Security Center*, *State Key Laboratory of Networking and Switching Technology*, *Beijing University of Posts and Telecommunications*, *Beijing* 100876, *China*)
(*Key Laboratory of Network and Information Attack & Defence Technology of MOE*, *Beijing University of Posts and Telecommunications*, *Beijing* 100876, *China*)
(*National Engineering Laboratory for Disaster Backup and Recovery*, *Beijing University of Posts and Telecommunications*, *Beijing* 100876, *China*)

Abstract: The concept of dynamic Distortion-Compensated Quantization Index Modulation (dynamic DC-QIM) is proposed, which differs from the conventional DC-QIM in whether or not quantization step size and DC parameter are changeable. Firstly, the condition satisfying the reversibility of dynamic DC-QIM is deduced. Then, the allowable range of DC parameter is derived. Finally, the procedure of reversible data hiding algorithm based on dynamic DC-QIM is designed. Its data hiding rate can achieve as high as 1bpp in a single iteration, higher than its former counterparts. Furthermore, the use of dynamic characteristic is in favor of preventing its parameters from being disclosed. Experimental results show that it not only accurately decodes the secret information, but also perfectly restores the original cover, regardless of initial conditions.

Key words: Information hiding; Dynamic Distortion-Compensated Quantization Index Modulation (dynamic DC-QIM); Reversible data hiding; Data hiding rate

1 引言

可逆数据隐藏是一种特殊的信息隐藏技术。它的目的在于不仅能够解码出秘密信息，而且还能准确恢复原始载体。设计可逆数据隐藏算法的关键在于发现和利用可逆性。例如，基本可逆对比映射算法[1]和它的改进算法[2]利用 ceil 函数的可逆性在像素对上实现正、反向变换。Eggers 等[3]首次发现标量 Costa 方法(SCS，和失真补偿量化索引调制 DC-QIM[4,5]等价)也存在某种可逆性。遗憾的是，他们仅仅从理论意义上发现可逆性的存在，但并未设计出具体的基于失真补偿量化索引调制的可逆数据隐藏算法。另一个问题是：传统失真补偿量化索引调制的量化步长和失真补偿(DC)参数是固定不变的，容易被泄露。本文提出了动态失真补偿量化索引调制

2009-06-09 收到，2009-11-24 改回
国家 973 计划项目(2007CB311203)，国家自然科学基金(60821001，U0835001，60803157)，高等学校博士学科点专项科研基金(20070013007)和高等学校学科创新引智计划(B08004)资助课题
通信作者：叶天语 flystu008@yahoo.com.cn

的概念。它和传统失真补偿量化索引调制的区别在于量化步长和失真补偿参数是否可变。本文推导出动态失真补偿量化索引调制可逆性的成立条件，并推导出失真补偿参数的可允许范围，最后利用可逆性设计一个具体的可逆数据隐藏算法。

2 失真补偿量化索引调制原理

首先简要回顾失真补偿量化索引调制的原理[3−5]。

令 x_n 代表原始载体，$b_n \in \{0,1\}$ 代表 1 bit 原始秘密信息，s_n 代表隐秘后的载体。传统失真补偿量化索引调制通常使用具有相同量化步长 Δ 的两个均匀标量量化器 Λ_0，Λ_1 进行量化。它们的量化中心分别位于

$$\Lambda_0(x_n) = k\Delta - \Delta/2,\ \ k \in Z \tag{1}$$

$$\Lambda_1(x_n) = k\Delta,\ \ k \in Z \tag{2}$$

在编码端，利用原始载体 x_n 通过以下规则产生隐秘载体 s_n：

$$s_n = x_n + \alpha[\Lambda_{b_n}(x_n) - x_n] = (1-\alpha)x_n + \alpha\Lambda_{b_n}(x_n) \tag{3}$$

其中 $\alpha \in [0,1]$ 是失真补偿参数。当 α 等于 1 时，失真补偿量化索引调制退化为一般的量化索引调制。因此，当后文提到失真补偿量化索引调制时，默认 α 不等于 1。

隐秘载体 s_n 一般会经历一系列失真，如噪声干扰等，解码端收到失真的隐秘载体 $\hat{s}_n$。在解码端，嵌入的秘密信息通常用最小距离解码器进行解码，即

$$\hat{b}_n = \arg\min_{0,1} \left\| s_n - \Lambda_{\hat{b}_n}(s_n) \right\|^2 \tag{4}$$

3 基于动态失真补偿量化索引调制可逆数据隐藏算法的可行性分析

在传统失真补偿量化索引调制中，量化步长和失真补偿参数是固定的。而本文提出的动态失真补偿量化索引调制则具有可变的量化步长和可变的失真补偿参数。

(1)动态失真补偿量化索引调制的可逆性　在编码端，原始载体 x_n 的量化误差定义为

$$q_n = \Lambda_{b_n}(x_n) - x_n \tag{5}$$

和传统失真补偿量化索引调制类似，在动态失真补偿量化索引调制中，隐秘载体 s_n 通过如下规则产生：

$$s_n = x_n + \alpha_n q_n = (1-\alpha_n)x_n + \alpha_n\Lambda_{b_n}(x_n) \tag{6}$$

其中失真补偿参数 α_n 随着不同的原始载体 x_n 而变化。由式(6)可以得到

$$x_n = \frac{s_n}{1-\alpha_n} - \frac{\alpha_n}{1-\alpha_n}\Lambda_{b_n}(x_n) \tag{7}$$

可逆数据隐藏一般应用在无噪环境，所以本文考虑无噪情况。解码端收到无失真隐秘载体 s_n。类似地，隐秘载体 s_n 的量化误差可定义为

$$q_n' = \Lambda_{b_n}(s_n) - s_n \tag{8}$$

另外，定义

$$x_n' = \Lambda_{b_n}(s_n) - \frac{q_n'}{1-\alpha_n} \tag{9}$$

将式(8)代入式(9)，得到

$$x_n' = \Lambda_{b_n}(s_n) - \frac{\Lambda_{b_n}(s_n) - s_n}{1-\alpha_n} = \frac{s_n}{1-\alpha_n} - \frac{\alpha_n}{1-\alpha_n}\Lambda_{b_n}(s_n) \tag{10}$$

比较式(7)和式(10)可以发现，只要满足以下条件，原始载体 x_n 就可以被准确地恢复出来：

$$\Lambda_{b_n}(x_n) = \Lambda_{b_n}(s_n) = \Lambda_{b_n}[(1-\alpha_n)x_n + \alpha_n\Lambda_{b_n}(x_n)] \tag{11}$$

本文称式(11)为动态失真补偿量化索引调制可逆性的成立条件。它的含义是：当隐秘载体的量化结果和原始载体的量化结果相同时，原始载体就可以被准确地恢复出来。

(2)失真补偿参数的可允许范围　接下来推导不同秘密信息 b_n 时满足式(11)的失真补偿参数 α_n 的可允许范围。

(a)当 $b_n = 0$，使用 Λ_0 进行量化

(a_1) 当 $x_n \in [k\Delta_n - \Delta_n/2, k\Delta_n]$ 时，满足式(11)将得到

$$k\Delta_n - \Delta_n \le (1-\alpha_n)x_n + \alpha_n(k\Delta_n - \Delta_n/2) \le k\Delta_n \tag{12}$$

移项后得到

$$k\Delta_n - \Delta_n - x_n \le \alpha_n(-x_n + k\Delta_n - \Delta_n/2) \le k\Delta_n - x_n \tag{13}$$

因为 $x_n \in [k\Delta_n - \Delta_n/2, k\Delta_n]$，所以

$$-\Delta_n/2 \le -x_n + k\Delta_n - \Delta_n/2 \le 0$$

由式(13)得到此时 α_n 的可允许范围为

$$1 + \frac{\Delta_n}{2(-x_n + k\Delta_n - \Delta_n/2)} \le \alpha_n \le 1 - \frac{\Delta_n}{2(-x_n + k\Delta_n - \Delta_n/2)} \tag{14}$$

(a_2) 当 $x_n \in (k\Delta_n, k\Delta_n + \Delta_n/2)$，满足式(11)将得到

$$k\Delta_n \le (1-\alpha_n)x_n + \alpha_n(k\Delta_n + \Delta_n/2) \le k\Delta_n + \Delta_n \tag{15}$$

既然 $x_n \in (k\Delta_n, k\Delta_n + \Delta_n/2)$，由式(15)得到此时 α_n 的可允许范围为

$$1 - \frac{\Delta_n}{2(-x_n + k\Delta_n + \Delta_n/2)} \le \alpha_n \le 1 + \frac{\Delta_n}{2(-x_n + k\Delta_n + \Delta_n/2)} \tag{16}$$

(b)当 $b_n = 1$，使用 Λ_1 进行量化

(b_1) 当 $x_n \in [k\Delta_n, k\Delta_n + \Delta_n/2]$，满足式(11)将得到

$$k\Delta_n - \Delta_n/2 \le (1-\alpha_n)x_n + \alpha_n k\Delta_n \le k\Delta_n + \Delta_n/2 \tag{17}$$

既然 $x_n \in [k\Delta_n, k\Delta_n + \Delta_n/2]$，由式(17)得到此时 α_n 的可允许范围为

$$1 + \frac{\Delta_n}{2(-x_n + k\Delta_n)} \le \alpha_n \le 1 - \frac{\Delta_n}{2(-x_n + k\Delta_n)} \tag{18}$$

(b_2) 当 $x_n \in (k\Delta_n + \Delta_n/2, k\Delta_n + \Delta_n)$，满足式(11)将得到

$$k\Delta_n + \Delta_n/2 \le (1-\alpha_n)x_n + \alpha_n(k\Delta_n + \Delta_n) \le k\Delta_n + 3\Delta_n/2 \tag{19}$$

既然 $x_n \in (k\Delta_n + \Delta_n/2, k\Delta_n + \Delta_n)$，由式(19)得到此时 α_n 的可允许范围为

$$1 - \frac{\Delta_n}{2(-x_n + k\Delta_n + \Delta_n)} \le \alpha_n \le 1 + \frac{\Delta_n}{2(-x_n + k\Delta_n + \Delta_n)} \tag{20}$$

由式(14)，式(16)，式(18)和式(20)可以得出如下结论：(1)在判断出 x_n 所处的区间后，只要 α_n 在可允许范围内选择，就可以利用隐秘载体准确恢复出原始载体。(2)经过一些简单的计算，可以很容易发现式(14)、式(16)、式(18)和式(20)的左边式子总是小于等于 0，而右边式子总是大于等于 2。因此，在动态失真补偿量化索引调制中，不管秘密信息 b_n 如何，失真补偿参数 α_n 都可以是一个负数。而在传统失真补偿量化索引调制中，α 必须是一个正数。(3)传统失真补偿量化索引调制的量化步长和失真补偿参数都是固定的，只要给定足够多的隐秘载体，它们将容易被推测出来。相对来说，在动态失真补偿量化索引调制中，由于不同的隐秘载体是通过不同的量化步长和失真补偿参数产生，所以想推测出它们将是困难的。

4　基于动态失真补偿量化索引调制可逆数据隐藏算法的实现步骤及数据隐藏率

(1)基于动态失真补偿量化索引调制可逆数据隐藏算法的实现步骤　下面分别详细叙述编码端和解码端的可逆数据隐藏算法实现步骤。

(a)编码端

(a_1) 使用步长为 Δ_n 的量化器 Λ_{b_n} 对原始载体 x_n 进行量化。

(a_2) 根据 b_n 和 x_n/Δ_n 所处的区间推导出 k。

(a_3) 根据式(14)，式(16)，式(18)和式(20)计算出 α_n 的可允许范围。

(a_4) 在 α_n 的可允许范围内为其随机选择一个值，并利用式(6)计算出隐秘载体 s_n。

与改进的可逆对比映射算法[2]创建一个查询表类似，本文也建立一个查询表来保存每个原始载体的量化步长 Δ_n 和失真补偿参数 α_n。查询表的每行可以表示成：

序列号 n；量化步长 Δ_n；失真补偿参数 α_n 可以进一步根据实际情况和要求采取一些特殊措施来减少查询表的存储量。例如，一种特殊方法是：不管原始载体如何，让每个原始载体的量化步长都取值相同。因此就不必在查询表中存储量化步长。而且，不同失真补偿参数的可允许范围可能部分重合，那么可以将相应的失真补偿参数取值相同，并将相应的序列号放在一起与同一个失真补偿参数一起保存。

(b)解码端

(b_1) 通过查询表查询原始载体 x_n 相应的量化步长 Δ_n 和失真补偿参数 α_n。

(b_2) 根据 s_n/Δ_n 所处的区间分别推导对应于量化器 Λ_0，Λ_1 的 k_0，k_1。分别通过式(1)和式(2)产生量化器 Λ_0，Λ_1 对 s_n 量化的结果。

(b_3) 利用最小距离解码器式(4)估计出 $\hat{b}_n$。$\Lambda_{\hat{b}_n}$ 是最后真正被用于量化 s_n 的量化器。

(b_4) 计算式(10)得到恢复出的原始载体。

(2)数据隐藏率　既然每个原始载体量化嵌入 1 bit 秘密信息，本文提出的可逆数据隐藏算法数据隐藏率等于 1 bit 每像素。然而，基本可逆对比映射算法[1]和它的改进算法[2]的数据隐藏率上限都等于 0.5 bit 每像素，圆形直方图插值算法[6]的数据隐藏率更低。因此，与这些算法相比，本文算法具有更高的数据隐藏率。本文算法的数据隐藏率高于可逆对比映射算法的原因是：它的可逆变换是在单个像素上进行，而可逆对比映射算法是在像素对上进行。为了增加数据隐藏率，本文算法可以连续多遍重复执行。

5　实验结果

首先，本文给出一个例子说明编码器端和解码器端的算法实现过程。假设 $x_n = 198$，$b_n = 1$ 和 $\Delta_n = 5$。所以，$x_n/\Delta_n = 39.6$。因此，得到 $k = 39$ 和 $\Lambda_1(x_n) = k\Delta_n + \Delta_n = 200$。然后，计算式(5)得到 $q_n = 2$。根据式(20)，可以得出 $-0.25 \le \alpha_n \le 2.25$。在可允许范围内选择 $\alpha_n = 0.8$。结果，编码端在计算式(6)后得到 $s_n = 199.6$。建立查询表保存 Δ_n 和 α_n。在解码端，首先从查询表中查询出 Δ_n 和 α_n。然后，得到 $s_n/\Delta_n = 39.92$。因此，可以得到 $k_0 = 40$，$k_1 = 39$，$\Lambda_0(s_n) = k_0\Delta_n - \Delta_n/2 = 197.5$ 和 $\Lambda_1(s_n) = k_1\Delta_n + \Delta_n = 200$。既然 $|s_n - \Lambda_1(s_n)|^2 < |s_n - \Lambda_0(s_n)|^2$，

根据最小距离解码器式(4)，解码出 $\hat{b}_n=1$。计算式(10)，得出 $x_n^{'}=198$。因此，已经成功地恢复出原始载体。本文还做了大量的不同初始 x_n，b_n 和 Δ_n 值情形下的实验。实验结果都一致地表明：不管初始条件如何，本文的算法既能正确解码出秘密信息，又能准确恢复原始载体。

在一些实际应用中，例如水印应用场合，数据隐藏所引发的原始载体视听觉改变往往被要求是不可察觉的。以图 1 的大小为 256×256 的灰度图像 Lena 为例。量化操作只在每个像素上执行一遍。根据式(6)，当量化步长 Δ_n 给定时，为了确保具有良好的不可见性，应该从可允许范围内选择一个绝对值足够小的失真补偿参数 α_n。在这种情况下，它的数据隐藏容量为 65536 bit，数据隐藏率为 1 bit 每像素。含水印图像如图 2 所示。原始图像和含水印图像之间的 PSNR 为 48.2762，因此它具有良好的不可见性。可以很容易从含水印图像正确解码出水印信息和准确恢复出原始图像。而且，在确保不可见性的前提下，本文算法可以连续多遍重复执行，以提高数据隐藏率。本文还对不同类型的图像进行了实验，实验结论都是一致的。

图 1 原始图像

图 2 含水印图像

6 结论

本文提出了动态失真补偿量化索引调制的概念。在推导出动态失真补偿量化索引调制可逆性的成立条件和失真补偿参数的可允许范围后，利用可逆性设计了一个可逆数据隐藏算法。在只执行一遍时，它的数据隐藏率高达 1 bit 每像素，高于可逆对比映射算法和圆形直方图插值算法。算法的动态特性有利于防止参数泄露。不管初始条件如何，该算法既能正确解码出原始秘密信息，又能准确恢复原始载体。

参 考 文 献

[1] Coltuc D and Tremeau A. Simple reversible watermarking schemes. Proc. SPIE: Security, Steganography, Watermarking of Multimedia Contents VII, San Jose, CA, Jan. 2005, Vol. 5681: 561–568.

[2] Coltuc D and Chassery J M. Very fast watermarking by reversible contrast mapping. *IEEE Signal Processing Letters*, 2007, 14(4): 255–258.

[3] Eggers J J, Bäuml R, and Tzschoppe R, *et al*.. Inverse mapping of SCS-watermarked data. Proc. Eleventh European Signal Processing Conference (EUSIPCO'2002), Toulouse, France, Sep. 2002, Vol. I: 59–62.

[4] Perez-Gonzalez F, Balado F, and Hernandez J R. Performance analysis of existing and new methods for data hiding with known-host information in additive channels. *IEEE Transactions on Signal Processing*, 2003, 51(4): 960–980.

[5] Pérez-Freire L, Comesaña P, and Pérez-González F. Detection in quantization-based watermarking: Performance and security issues. Proc. SPIE: Security, Steganography, Watermarking of Multimedia Contents VII, San Jose, CA, Jan. 2005, Vol. 5681: 721–733.

[6] Vleeschouwer C D, Delaigle J F, and Macq B. Circular interpretation of bijective transformations in lossless watermarking for media asset management. *IEEE Transactions on Multimedia*, 2003, 5(1): 97–105.

叶天语： 男，1982年生，博士生，研究方向为信息隐藏与数字水印.

钮心忻： 女，1963年生，教授，博士生导师，研究方向为信号与信息处理、信息隐藏、数字水印等.

马兆丰： 男，1974年生，博士，主要研究方向为数字版权管理、数字内容安全、计算机网络安全.

杨义先： 男，1961年生，长江学者特聘教授，博士生导师，研究方向为密码学、计算机网络与信息安全等.