一种基于图像矢量量化压缩的数据隐藏方法

邱应强 张育钊 郭荣新 杜吉祥
(华侨大学信息科学与工程学院, 泉州 362021)

摘 要 根据码书中所有码字之间的最近邻关系,采用最近邻方法标记码书使得所有码字与其最近邻码字的标记值不同。在此基础上,运用 $\boldsymbol{I}/\bar{\boldsymbol{I}}$ 矩阵运算可在矢量量化压缩图像的每 $n=2m$ 个码字索引中有选择地最多修改 $\left\lfloor\frac{m}{2}\right\rfloor$ 个从而嵌入 m 比特数据。计算机上的仿真实验结果表明:该方法不仅具有较大的嵌入容量,而且具有较好的隐蔽性,可用于矢量量化压缩图像中的信息隐藏。

关键词 数据隐藏 矢量量化 最近邻方法 $\boldsymbol{I}/\bar{\boldsymbol{I}}$ 矩阵
中图法分类号: TP391 **文献标识码**: A **文章编号**: 1006-8961(2009)06-1096-06

Data Hiding Method Based on VQ_Compressed Images

QIU Ying-qiang, ZHANG Yu-zhao, GUO Rong-xin, DU Ji-xiang
(*College of Information Science & Engineering*, *Huaqiao University*, *Quanzhou* 362021)

Abstract According to the nearest relationship, the labeled value of every codeword in the labeled codebook by the nearest neighbor method was different from its nearest codeword, based on which, using $\boldsymbol{I}/\bar{\boldsymbol{I}}$ matrix, as many as m bits data can be embedded by selectively changing at most $\left\lfloor\frac{m}{2}\right\rfloor$ indexes in every $n=2m$ VQ_compressed indexes. The simulated results by the computer showed that the method used for information hiding in VQ_compressed images has larger capacity and better secrecy.

Keywords data hiding, vector quantization, nearest neighbor method, $\boldsymbol{I}/\bar{\boldsymbol{I}}$ matrix

1 引 言

信息隐藏[1]是一项新的信息安全技术,近年来得到了迅速的发展,可广泛应用于数字信息的版权保护、认证、机密信息的隐秘传输等领域。

当前,信息隐藏较多采用的空域方法[2]或变换域方法[3]是通过在空域或变换域中直接修改宿主信息实现数据嵌入,这些方法不能直接应用到矢量量化压缩数据中的信息隐藏。为此,结合矢量量化技术特点,出现了许多通过修改码字索引嵌入数据的方法[4-7]。这类方法先用“0”,“1”值标记矢量量化码书码字,然后采用奇偶调制方式使得码字索引标记值与当前嵌入数位值相同,从而嵌入数据。奇偶调制方法具有较高的数据嵌入容量,可在 n 个码字索引中嵌入 n 比特数据,但该方法嵌入数据后可能导致 n 个码字索引均不是全码书中的最佳码字,这将极大影响嵌入数据的隐蔽性。

2004 年,文献[8]给出了一种新颖的数据隐藏算法,将其推广到矢量量化压缩域中,可在 $n=2^m-1$ 个码字索引中最多修改 1 个,实现其中嵌入 m 比特数据[9],该方法提高了隐蔽性,但嵌入数据量较少;2005 年,程提出了多数位数据隐藏算法[10-11],若将该算法推广到矢量量化压缩域中则可实现在 $n=m+1$ 个码字索引中最多修改 $\left\lfloor\frac{m}{2}\right\rfloor$ 个($\lfloor\cdot\rfloor$ 代表向下

基金项目:福建省青年科技人才创新项目(2006F30086);华侨大学科研基金项目(06BS217,07HZR28)
收稿日期:2007-01-25;**改回日期**:2007-09-28

第一作者简介:邱应强(1981~),男。华侨大学信息科学与工程学院讲师,2006 年于中国科学技术大学获电路与系统专业硕士学位。研究方向为信息隐藏、图像处理等。E-mail:yqqiu@hqu.edu.cn

取整,下同)从而嵌入 m 比特数据,该算法嵌入数据量接近于奇偶调制方法,同时在隐蔽性上较之也有一定的提高。

本文将综合考虑数据嵌入容量和隐蔽性,给出一种基于图像矢量量化码字索引修改的数据隐藏新方法。该方法结合码书特点,采用最近邻方法标记码书,使得所有码字与其最近邻码字之间具有不同的标记值;并用 $\boldsymbol{I}/\overline{\boldsymbol{I}}$ 矩阵做嵌入/提取矩阵,在矢量量化压缩图像的每 $n=2m$ 个码字索引中,有选择地最多修改$\lfloor \frac{m}{2} \rfloor$个即可嵌入 m 比特数据。在计算机上进行了仿真实验,结果表明该方法不仅具有较大的信息嵌入量,而且具有较好的隐蔽性。

2　标记码书

由于图像矢量量化编码索引对应码字是全码书中的最佳匹配码字,而通过具有不同标记值的码字索引替换原码字索引,从而嵌入一定量的数据时势必引入失真。为了减少失真,要求不同标记值码字之间具有更大相似度。通常,标记码书采用按码书中各码字的模值或均值大小顺序标记“0”,“1”值的模排序方法、均值排序方法,或重复运用最近邻规则,在码书未标记码字中找到一对最近邻码字分别标记“0”,“1”值的最近邻对方法[9]。这几种方法标记码书能够使不同标记值码字之间具有一定的相似度,但如果所有码字与其最近邻码字之间标记值不同,那么不同标记值码字之间将具有更大的相似度。下面将结合码书码字之间的最近邻关系特点,给出一种新的码书标记方法——最近邻方法。

2.1　码书最近邻拓扑结构

对码书 $\boldsymbol{C}$(大小为 N)中的任一码字 $\boldsymbol{y}_k$,在 $\boldsymbol{C}$ 中可以找到一个码字 $\boldsymbol{y}_l$ 满足:

$$d(\boldsymbol{y}_k,\boldsymbol{y}_l)=\min_{1\leqslant j\leqslant N-1,j\neq k} d(\boldsymbol{y}_k,\boldsymbol{y}_j) \tag{1}$$

则称 $\boldsymbol{y}_l$ 为 $\boldsymbol{y}_k$ 的最近邻码字。如果有多个码字 $\boldsymbol{y}_{l_1}$,$\boldsymbol{y}_{l_2}$,…,$\boldsymbol{y}_{l_n}$均与 $\boldsymbol{y}_k$ 失真测度相同且最小时,则只有其中码字索引值最小的码字定义为 $\boldsymbol{y}_k$ 的最近邻码字。根据定义可知,一个码字的最近邻码字有且只有一个,但某些码字可能是多个码字的最近邻码字。因此,码书中的任意两个码字 $\boldsymbol{y}_k$,$\boldsymbol{y}_l$ 可能的最近邻关系有以下三种:

(1)双向最近邻关系

如果两个码字 $\boldsymbol{y}_k$, $\boldsymbol{y}_l$ 满足:

$$d(\boldsymbol{y}_k,\boldsymbol{y}_l)=\min_{1\leqslant i\leqslant N-1,i\neq l} d(\boldsymbol{y}_i,\boldsymbol{y}_l)=\min_{1\leqslant j\leqslant N-1,j\neq k} d(\boldsymbol{y}_k,\boldsymbol{y}_j) \tag{2}$$

即 $\boldsymbol{y}_k$、$\boldsymbol{y}_l$ 互为最近邻码字,可称 $\boldsymbol{y}_k$、$\boldsymbol{y}_l$ 双向最近邻,并用拓扑图 $\boldsymbol{y}_k \leftrightarrow \boldsymbol{y}_l$ 表示。

(2)单向最近邻关系

如果两个码字 $\boldsymbol{y}_k$,$\boldsymbol{y}_l$ 之间满足:

$$d(\boldsymbol{y}_k,\boldsymbol{y}_l)=\min_{1\leqslant j\leqslant N-1,j\neq k} d(\boldsymbol{y}_k,\boldsymbol{y}_j)>\min_{1\leqslant i\leqslant N-1,i\neq l} d(\boldsymbol{y}_i,\boldsymbol{y}_l) \tag{3}$$

即 $\boldsymbol{y}_l$ 为 $\boldsymbol{y}_k$ 的最近邻码字,但 $\boldsymbol{y}_l$ 的最近邻码字却不是 $\boldsymbol{y}_k$,则称 $\boldsymbol{y}_k$ 单向最近邻于 $\boldsymbol{y}_l$,拓扑图表示为 $\boldsymbol{y}_k \longrightarrow \boldsymbol{y}_l$。

(3)非最近邻关系

码字 $\boldsymbol{y}_l$,$\boldsymbol{y}_k$ 之间不存在以上任何一种最近邻关系。

根据码书中任意两个码字之间的最近邻关系,可以得到码书最近邻关系拓扑图,该拓扑图中一定不存在形如图 1 的环形结构。

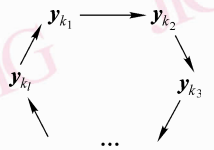

图 1　环形结构

Fig. 1　Annularity structure

因为根据最近邻关系的定义有

$$\begin{aligned} d(\boldsymbol{y}_{k_1},\boldsymbol{y}_{k_2}) &\geqslant d(\boldsymbol{y}_{k_2},\boldsymbol{y}_{k_3})\geqslant\cdots\geqslant d(\boldsymbol{y}_{k_{l-1}},\boldsymbol{y}_{k_l}) \\ &\geqslant d(\boldsymbol{y}_{k_l},\boldsymbol{y}_{k_1}) \end{aligned} \tag{4}$$

则 $d(\boldsymbol{y}_{k_1},\boldsymbol{y}_{k_2})\geqslant d(\boldsymbol{y}_{k_l},\boldsymbol{y}_{k_1})$,同时根据最近邻关系的定义可以推出 $k_2>k_l$,因此 $\boldsymbol{y}_{k_1}$最近邻于 $\boldsymbol{y}_{k_l}$,这与图 1 所示的 $\boldsymbol{y}_{k_1}$的最近邻码字是 $\boldsymbol{y}_{k_2}$相矛盾。因此,码书最近邻拓扑图中不存在环形结构。其基本结构如图 2 所示,其中码字 $\boldsymbol{y}_{k_6}$,$\boldsymbol{y}_{k_7}$,$\boldsymbol{y}_{k_8}$,$\boldsymbol{y}_{k_9}$不为任何码字的最近邻码字,可称为端点码字;$\boldsymbol{y}_{k_3}$,$\boldsymbol{y}_{k_4}$,$\boldsymbol{y}_{k_5}$, $\boldsymbol{y}_{k_{10}}$,$\boldsymbol{y}_{k_{11}}$,$\boldsymbol{y}_{k_{12}}$为某些码字的最近邻码字,但不与任何码字之间构成双向最近邻关系,可称为过渡码字;而 $\boldsymbol{y}_{k_1}$与 $\boldsymbol{y}_{k_2}$之间构成双向最近邻关系,称为终结码字对。在码书中可能存在不止一个终结码字对,因此码书拓扑图中存在多个形如图 2 的树状拓扑结构。

2.2　最近邻方法标记码书

设 $\boldsymbol{C}$ 代表大小为 N 的码书,$\boldsymbol{C}_{-1}$为所有未标记码字集合,$\boldsymbol{C}_0$ 为标记值为“0”的码字集合,$\boldsymbol{C}_1$ 为标记值为“1”的码字集合。最近邻方法标记码书实现

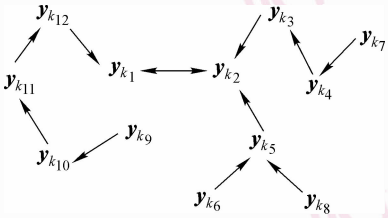

图 2 基本拓扑结构

Fig. 2 Basic topological structure

步骤如下:

第 1 步:初始化 $\boldsymbol{C}_{-1}=\boldsymbol{C},\boldsymbol{C}_0=\boldsymbol{C}_1=\boldsymbol{\phi}$。

第 2 步:从未标记码字集合 $\boldsymbol{C}_{-1}$ 中找到所有满足双向最近邻关系的码字 $\boldsymbol{y}_k,\boldsymbol{y}_l(k\neq l)$:

$$d(\boldsymbol{y}_k,\boldsymbol{y}_l)=\min_{0\leqslant m,n\leqslant N-1且m\neq n} d(\boldsymbol{y}_m,\boldsymbol{y}_n) \tag{5}$$

将所有终结码字对 $\boldsymbol{y}_k,\boldsymbol{y}_l$ 从集合 $\boldsymbol{C}_{-1}$ 中删除,分别赋予标记值“0”,“1”,然后分别归并到集合 $\boldsymbol{C}_0$,$\boldsymbol{C}_1$ 中。

第 3 步:分别从集合 $\boldsymbol{C}_{-1}$,集合($\boldsymbol{C}_0\bigcup\boldsymbol{C}_1$)中各选取一个码字 $\boldsymbol{y}_k\in\boldsymbol{C}_{-1},\boldsymbol{y}_l\in(\boldsymbol{C}_0\bigcup\boldsymbol{C}_1)$,要求满足:

$$d(\boldsymbol{y}_k,\boldsymbol{y}_l)=\min_{\boldsymbol{y}_m\in\boldsymbol{C}_{-1},\boldsymbol{y}_n\in(\boldsymbol{C}_0\bigcup\boldsymbol{C}_1)} d(\boldsymbol{y}_m,\boldsymbol{y}_n) \tag{6}$$

将码字 $\boldsymbol{y}_k$ 从集合 $\boldsymbol{C}_{-1}$ 中删除。若 $\boldsymbol{y}_l\in\boldsymbol{C}_0$,则赋予 $\boldsymbol{y}_k$ 标记值“1”,然后归并到集合 $\boldsymbol{C}_1$ 中;反之,有 $\boldsymbol{y}_l\in\boldsymbol{C}_1$,则赋予 $\boldsymbol{y}_k$ 标记值“0”,再归并到集合 $\boldsymbol{C}_0$ 中。

第 4 步:若 $\boldsymbol{C}_{-1}=\phi$,则完成了所有码字标记。否则,转向第 3 步。

根据码书拓扑图特点,第 2 步选取所有终点码字对并分别标记“0”、“1”值,在标记完所有终结码字对的基础上,第 3 步将通过已标记码字与未标记码字之间存在的单向最近邻关系标记每一个未标记码字,结果满足单向最近邻关系的两个码字将具有不同标记值。因此,上述步骤标记码书可实现任意码字与其最近邻码字的标记值不同,从而提高不同标记值码字之间的相似度。

3 数据嵌入/提取算法

3.1 算法概述

算法主要包括数据嵌入、数据提取两大部分。算法在数据嵌入/提取过程中需要运用一个大小为 $m\times 2m$ 的嵌入/提取矩阵:

$$\boldsymbol{U}=[\boldsymbol{u}_1,\boldsymbol{u}_2,\cdots,\boldsymbol{u}_{2m}]$$

$$=\begin{bmatrix} 1 & 0 & \cdots & 0 & 0 & 1 & \cdots & 1 \\ 0 & 1 & \cdots & 0 & 1 & 0 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & 1 & 1 & \cdots & 0 \end{bmatrix}_{m\times 2m} \tag{7}$$

该矩阵由一个 m 阶($m\geqslant 3$)的单位矩阵 $\boldsymbol{I}$,加上满足式(8)的一个 m 阶方阵 $\bar{\boldsymbol{I}}=(\alpha_{ij})_{m\times m}$ 组成,可称之为 $\boldsymbol{I}/\bar{\boldsymbol{I}}$ 矩阵。

$$\alpha_{ij}=\begin{cases}0 & i=j\\ 1 & i\neq j\end{cases} \tag{8}$$

数据嵌入如图 3 所示:为了实现在矢量量化压缩的图像信息中嵌入数据,先采用最近邻方法标记码书;根据已标记码书,将每 $2m$ 个图像块的 VQ 编码索引标记值组成 $2m$ 维的二值标记向量 $\boldsymbol{a}=(a_1,a_2,\cdots,a_{2m})$,同时将每 m 比特待嵌入数据组成 m 维数据向量 $\boldsymbol{b}=(b_1,b_2,\cdots,b_m)$;根据向量 $\boldsymbol{a},\boldsymbol{b}$ 信息,通过 $\boldsymbol{I}/\bar{\boldsymbol{I}}$ 矩阵运算可确定几种可行的最多修改$\lfloor\frac{m}{2}\rfloor$个码字索引的位置组合;对其中引入总失真最小的位置组合,原索引用标记值不同且最近邻码字索引替代,即可完成在 $2m$ 个码字索引中嵌入 m 比特数据。

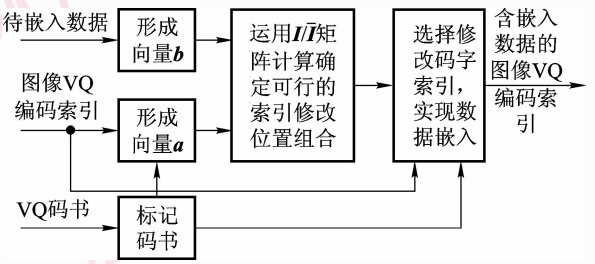

图 3 数据嵌入原理框图

Fig. 3 Block diagram of data embedding

嵌入信息的提取,则根据含嵌入数据的图像 VQ 编码索引流中的每 $2m$ 个码字索引标记值组成的向量 $\boldsymbol{z}=(z_1,z_2,\cdots,z_{2m})$,通过 $\boldsymbol{I}/\bar{\boldsymbol{I}}$ 矩阵运算得到其中的 m 比特嵌入数据。

3.2 数据嵌入/提取算法原理

令

$$\boldsymbol{c}=\boldsymbol{b}^{\mathrm{T}}\oplus\boldsymbol{U}\boldsymbol{a}^{\mathrm{T}}$$

$$=\begin{bmatrix} b_1\oplus u_{11}\cdot a_1\oplus u_{12}\cdot a_2\oplus\cdots\oplus u_{1(2m)}a_{2m} \\ b_1\oplus u_{21}\cdot a_1\oplus u_{22}\cdot a_2\oplus\cdots\oplus u_{2(2m)}a_{2m} \\ \vdots \\ b_1\oplus u_{m1}\cdot a_1\oplus u_{m2}\cdot a_2\oplus\cdots\oplus u_{m(2m)}a_{2m} \end{bmatrix} \tag{9}$$

式中“$\oplus$”为异或运算(下同),得到 m 维二值列向

量 $\boldsymbol{c}=(c_1,c_2,\cdots,c_m)^{\mathrm{T}}$。

若 $\boldsymbol{c}$ 中“1”的个数 $l=0$,即 $\boldsymbol{c}$ 为零向量,有 $\boldsymbol{b}^{\mathrm{T}}=\boldsymbol{U}\boldsymbol{a}^{\mathrm{T}}$,无需修改 $2m$ 个码字索引即可嵌入 m 比特数据,此时 $\boldsymbol{z}=\boldsymbol{a}$,$\boldsymbol{b}^{\mathrm{T}}=\boldsymbol{U}\boldsymbol{z}^{\mathrm{T}}$。

若 $\boldsymbol{c}$ 不为零向量时,根据 $\boldsymbol{c}$ 中值为“1”的元素个数做如下讨论:

(1)若 $\boldsymbol{c}$ 中“1”的个数 $1\leqslant l\leqslant L\left(L=\left\lfloor\frac{m}{2}\right\rfloor\right)$时,不妨设 c_{i_1}、c_{i_2},$\cdots$,$c_{i_l}(1\leqslant i_1,i_2,\cdots,i_l\leqslant m)$值为“1”,则对 $\boldsymbol{c}$ 中每一个值为“1”的行,可在 $\boldsymbol{I}/\bar{\boldsymbol{I}}$ 矩阵前 m 列子阵 $\boldsymbol{I}$ 中找到唯一的相应行值为“1”的列向量,共 l 个列向量 $\boldsymbol{u}_{i_1},\boldsymbol{u}_{i_2},\cdots,\boldsymbol{u}_{i_l}$,使得:

$$\boldsymbol{c}=\boldsymbol{u}_{i_1}\oplus\boldsymbol{u}_{i_2}\oplus\cdots\oplus\boldsymbol{u}_{i_l}\tag{10}$$

(2)若 $\boldsymbol{c}$ 中“1”的个数 $L+1\leqslant l\leqslant m-1$ 时,其中值为“0”的元素个数 $0\leqslant j\leqslant L$,不妨设 $\boldsymbol{c}$ 中 c_{i_1},c_{i_2},$\cdots$,$c_{i_j}(1\leqslant i_1,i_2,\cdots,i_j\leqslant m)$值为“0”,其余值为“1”。由于子阵 $\bar{\boldsymbol{I}}$ 中每行有且只有一个“0”,可从该子阵中选取一列向量,满足列向量 $\boldsymbol{c}$ 在该列向量“0”值所在行的值也为“0”,不妨设该列向量为 $\boldsymbol{u}_{i_1+m}(1\leqslant i_1\leqslant m)$,而对 $\boldsymbol{c}$ 中其余值为“0”的行,在子阵 $\boldsymbol{I}$ 中找到唯一的相应行值为“1”的列向量,分别为 $\boldsymbol{u}_{i_2},\cdots,\boldsymbol{u}_{i_j}$。这 j 个列向量 $\boldsymbol{u}_{i_1+m},\boldsymbol{u}_{i_2},\cdots,\boldsymbol{u}_{i_j}(1\leqslant i_1,i_2,\cdots,i_j\leqslant m)$满足:

$$\boldsymbol{c}=\boldsymbol{u}_{i_1+m}\oplus\boldsymbol{u}_{i_2}\oplus\cdots\oplus\boldsymbol{u}_{i_j}\tag{11}$$

式中,仅有的一个选自子阵 $\bar{\boldsymbol{I}}$ 的列向量可以为 $\boldsymbol{u}_{i_2+m},\cdots,\boldsymbol{u}_{i_j+m}$ 中的任何一个,$\boldsymbol{c}$ 有 j 种不同的表达形式。

(3)若 $\boldsymbol{c}$ 中 $c_1,c_2,\cdots,c_m$ 的值全为“1”(共 m 个),则 $\boldsymbol{c}$ 有 m 种不同的表达形式。

$$\boldsymbol{c}=\boldsymbol{u}_i\oplus\boldsymbol{u}_{i+m},1\leqslant i\leqslant m\tag{12}$$

因此,任意元素不全为零的 m 阶二值列向量 $\boldsymbol{c}$,都可在 $\boldsymbol{I}/\bar{\boldsymbol{I}}$ 矩阵中找到一组不超过 $L=\left\lfloor\frac{m}{2}\right\rfloor$ 个列向量 $\boldsymbol{u}_{n_1},\cdots,\boldsymbol{u}_{n_k}(1\leqslant n_1,\cdots,n_k\leqslant 2m$ 且 $k\leqslant L)$,满足:

$$\boldsymbol{c}=\boldsymbol{u}_{n_1}\oplus\boldsymbol{u}_{n_2}\oplus\cdots\oplus\boldsymbol{u}_{n_k}\tag{13}$$

相应地,第 $\boldsymbol{u}_{n_1},\boldsymbol{u}_{n_2},\cdots,\boldsymbol{u}_{n_k}$ 个码字索引用与其最近邻且标记值不同的码字索引替代,从而嵌入 m 比特数据。此时,$2m$ 个码字索引标记值向量 $\boldsymbol{z}=(a_1,\cdots,a_{n_1}\oplus 1,\cdots,a_{n_k}\oplus 1,\cdots,a_{2m})$,根据

$$\begin{aligned}\boldsymbol{U}\boldsymbol{z}^{\mathrm{T}}&=\boldsymbol{u}_1a_1\oplus\cdots\oplus\boldsymbol{u}_{n_1}(a_{n_1}\oplus 1)\oplus\cdots\oplus\\&\quad\boldsymbol{u}_{n_k}(a_{n_k}\oplus 1)\oplus\cdots\oplus\boldsymbol{u}_{2m}a_{2m}\\&=(\boldsymbol{u}_1a_1\oplus\boldsymbol{u}_2a_2\oplus\cdots\oplus\boldsymbol{u}_{2m}a_{2m})\\&\quad\oplus(\boldsymbol{u}_{n_1}\oplus\boldsymbol{u}_{n_2}\oplus\cdots\oplus\boldsymbol{u}_{n_k})\\&=\boldsymbol{U}\boldsymbol{a}^{\mathrm{T}}\oplus\boldsymbol{c}^{\mathrm{T}}=\boldsymbol{b}^{\mathrm{T}}\end{aligned}\tag{14}$$

可得 $\boldsymbol{b}^{\mathrm{T}}=\boldsymbol{U}\boldsymbol{z}^{\mathrm{T}}$。

因此,提取嵌入信息时只需计算 $\boldsymbol{b}^{\mathrm{T}}=\boldsymbol{U}\boldsymbol{z}^{\mathrm{T}}$ 即可。

3.3　$\boldsymbol{I}/\bar{\boldsymbol{I}}$ 矩阵的选择性

在 3.2 节中已经讨论得出式(11)、式(12)分别有 j,m 种不同的表达形式。此外,由于在子阵 $\boldsymbol{I}$ 中的任意两个列向量异或运算等于子阵 $\bar{\boldsymbol{I}}$ 中相应列向量异或运算的结果,即

$$\boldsymbol{u}_i\oplus\boldsymbol{u}_j=\boldsymbol{u}_{m+i}\oplus\boldsymbol{u}_{m+j}(1\leqslant i,j\leqslant m\text{ 且 }i\neq j)\tag{15}$$

式(13)中任意偶数个选自子阵 $\boldsymbol{I}$ 中列向量可以用子阵 $\bar{\boldsymbol{I}}$ 中相应的列向量同时替代,式(13)依然成立。因此,式(13)中 $\boldsymbol{c}$ 的不同表达形式数为

(1)当 $1\leqslant l\leqslant L$ 时

$$Nums=\sum_{i=0,i=i+2}^{2\times\left\lfloor\frac{l}{2}\right\rfloor}\boldsymbol{C}_l^i$$

$$2\times\left\lfloor\frac{l}{2}\right\rfloor=\begin{cases}l-1 & l\text{ 为奇数}\\ l & l\text{ 为偶数}\end{cases}$$

其中,l 为 $\boldsymbol{C}$ 中值为“1”的元素个数。

(2)当 $L+1\leqslant l\leqslant m-1$ 时

$$Nums=\sum_{i=1,i=i+2}^{2\times\left\lceil\frac{j}{2}\right\rceil-1}\boldsymbol{C}_j^i$$

$$2\times\left\lceil\frac{j}{2}\right\rceil-1=\begin{cases}j & j\text{ 为奇数}\\ j-1 & j\text{ 为偶数}\end{cases}$$

其中,$\lceil\cdot\rceil$为向上取整,$j=m-t$ 为 $\boldsymbol{C}$ 中值为“0”的元素个数。

(3)特别地,当 $\boldsymbol{c}$ 中“0”,“1”元素个数相同(即 m 为偶数且 $l=j$)时,c 既可按(1)处理,也可按(2)处理。

$$Nums=\sum_{i=0,i=i+2}^{2\times\left\lfloor\frac{l}{2}\right\rfloor}\boldsymbol{C}_l^i+\sum_{i=1,i=i+2}^{2\times\left\lceil\frac{j}{2}\right\rceil-1}\boldsymbol{C}_j^i=\sum_{i=0}^{l}\boldsymbol{C}_l^i$$

4)当 $l=m$ 时,$Nums=m$

表 1 给出了 m 分别为 8,12,16,$\boldsymbol{c}$ 中元素“1”个数不同时,$\boldsymbol{c}$ 的不同表达形式数。由于 $\boldsymbol{c}$ 的任何一种表达形式都对应于一种索引修改位置组合,因此通过 $\boldsymbol{I}/\bar{\boldsymbol{I}}$ 矩阵的选择性有选择地修改码字索引,可减小引入的失真。

表 1 c 中元素“1”个数 l 不同时 c 的不同表达形式数

Tab. 1 The number of c's different forms according to different number of element “l” in c

l	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$m=8$	1	2	4	16	4	2	1	4	—	—	—	—	—	—	—	—
$m=12$	1	2	4	8	16	64	16	8	4	2	1	6	—	—	—	—
$m=16$	1	2	4	8	16	32	64	256	64	32	16	8	4	2	1	8

4 仿真实验及数据分析

为了验证本文方法,在计算机(Windows 2000 平台)上用软件 Visual C ++ 6.0 和 Matlab 7.0 进行了仿真实验。实验在采用大小为 512 的码书(矢量为 4 × 4 图像块)对 512 × 512 的 256 级灰度图像 Lena,Pepper,Plane 及 Goldhill 矢量量化压缩的基础上,嵌入一定量的汉字信息。并用嵌入数据前、后 VQ 解码图像间的峰值信噪比来客观评估算法性能。

4.1 各种码书标记方法的比较

实验采用各种不同的码书标记方法标记码书,并用提出的大小为 32 × 64 的 $\boldsymbol{I}/\bar{\boldsymbol{I}}$ 矩阵,分别在这 4 幅图像 VQ 编码的数据中嵌入大小为 8 192 比特的汉字信息。嵌入数据前后 VQ 解码图像间的峰值信噪比如表 2 所示。从实验数据中可以得到,最近邻方法略优于模排序方法、均值排序方法和最近邻对方法。图 4 给出了部分实验示意图。

表 2 不同标记方法实现信息隐藏前、后 VQ 解码图像之间的峰值信噪比

Tab. 2 PSNR between VQ decoded images with and without data hidden by different labeling methods

(单位:dB)

码书标记方法	Lena	pepper	plane	goldhill
模排序方法	43.17	41.58	41.01	41.58
均值排序方法	43.00	41.09	40.47	41.51
最近邻对方法	43.55	42.23	41.48	41.95
最近邻方法	43.72	42.58	41.64	42.10

(a) Lena的VQ解码图 (b) 模排序方法 (c) 均值排序方法 (d) 最近邻对方法 (e) 最近邻方法

图 4 用各种码书标记方法实现数据嵌入后的 VQ 解码示意图

Fig. 4 VQ decoded images with data embedded by some codebook labeling method

4.2 各种数据嵌入算法的比较

实验采用最近邻方法标记的码书,分别用奇偶调制算法、文献[8]~[9]中使用的数据隐藏算法 1(嵌入/提取矩阵大小为 4 × 16)、文献[10]~[11]中采用的数据隐藏算法 2(嵌入/提取矩阵大小为 15 × 16)及本文给出的 $\boldsymbol{I}/\bar{\boldsymbol{I}}$ 矩阵嵌入算法(嵌入/提取矩阵大小为 32 × 64)实现数据隐藏来比较各种数据嵌入算法。表 3 给出了这几种数据嵌入算法得到的峰值信噪比:奇偶调制算法嵌入数据量最大,但算法对数据嵌入后的图像质量影响较大;数据隐藏算法 2 同样具有较大的数据嵌入量,数据嵌入后的图像质量较奇偶调制算法有一定的提高;虽然 $\boldsymbol{I}/\bar{\boldsymbol{I}}$ 矩

表 3 不同嵌入算法实现数据嵌入前、后 VQ 解码图像之间的峰值信噪比

Tab. 3 PSNR between VQ decoded images with and without data hidden by different embedded algorithms

(单位:dB)

嵌入算法	嵌入数据量(bits)	Lena	pepper	plane	goldhill
奇偶调制	16 384	35.72	34.18	32.64	34.58
算法 1	4 096	45.03	43.69	42.20	44.21
算法 2	15 360	36.71	35.28	33.27	35.60
$\boldsymbol{I}/\bar{\boldsymbol{I}}$ 矩阵	8 192	43.72	42.58	41.64	42.10

阵嵌入算法嵌入数据量只有前两种算法的一半左右,但嵌入数据前、后图像间的平均峰值信噪比较前两种算法分别提高了 8.2 dB、7.3 dB,且仅比嵌入信息量只有该算法一半的数据隐藏算法 1 低 1.3 dB。

4.3 $I/\bar{I}$ 矩阵选择性实验

$I/\bar{I}$ 矩阵做嵌入/提取矩阵时,对码字索引的修改具有一定的选择性,表 4 给出了分别用大小为 16×32,32×64,64×128 的 $I/\bar{I}$ 矩阵通过最优修改组合及其中一种修改组合实现数据嵌入前后 VQ 解码图像之间的峰值信噪比。从实验数据可以看出,随着 $I/\bar{I}$ 矩阵的增大,采用非最优修改码字索引实现数据嵌入后图像质量会有所下降,而采用 $I/\bar{I}$ 矩阵选择最优修改位置可以大大减少嵌入信息所引入的失真。$I/\bar{I}$ 矩阵的选择性使得嵌入数据前、后图像间的平均峰值信噪比至少提高了 3 dB,这也是在矢量量化压缩图像的数据隐藏中该算法隐蔽性优于其他算法的缘由。

以上实验,嵌入数据均能 100% 正确提取。

表 4　$I/\bar{I}$ 矩阵选择性对图像峰值信噪比的影响

Tab. 4　The effect to PSNR by the selectivity of $I/\bar{I}$ matrix　(单位:dB)

矩阵大小	修改方式	Lena	pepper	plane	goldhill
16×32	最优	43.37	41.81	41.81	42.02
	非最优	40.40	38.65	36.83	38.80
32×64	最优	43.72	42.58	41.64	42.10
	非最优	40.11	38.71	36.77	38.94
64×128	最优	43.89	42.82	41.64	41.67
	非最优	39.32	37.22	36.39	38.04

5　结　论

本文提出了一种在矢量量化压缩图像中的数据隐藏新方法。方法采用最近邻方法对码书码字标记“0”,“1”值,使得所有码字与其最近邻码字具有不同的标记值,提高了不同标记值码字之间的相似度。同时,采用 $I/\bar{I}$ 矩阵做嵌入/提取矩阵,可实现在矢量量化压缩图像的每 $n=2m$ 个码字索引中有选择地最多修改 $\lfloor\frac{m}{2}\rfloor$ 个从而嵌入 m 比特信息。仿真实验结果表明:该方法不仅具有较大数据嵌入容量,而且具有较好的隐蔽性,在一定程度上缓解了存在信息隐藏中的嵌入数据容量与嵌入数据隐蔽性之间的矛盾。

参考文献(References)

1　Moulin P, Sullivan J O. Information-theoretic analysis of information hiding[J]. IEEE Transactions on Information theory, 2003, **49**(3): 563-593.

2　Mukherjee D P, Maitra S, Acton S T. Spatial domain digital watermarking of multimedia objects for buyer authentication[J]. IEEE Transactions on Multimedia, 2004, **6**(1): 1-15.

3　Bao P, Ma X H. Image adaptive watermarking using wavelet domain singular value decomposition[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2005, **15**(1): 96-102.

4　Lu Z M, Sun S H. Digital image watermarking technique based on vector quantisation[J]. Electronics Letters, 2000, **36**(4): 303-305.

5　Wu X, Lu Z M, Wang H X. A Digital watermarking method based on classified labeled-bisecting-k-means clustering[A]. In: Proceedings of The International Conference on Machine Learning and Cybernetics [C], Xi'an, 2003, **5**(5): 2891-2895.

6　Lu Z M, Xing W, Xu D G, *et al*. Digital image watermarking method based on vector quantization with labeled codewords[J]. IEICE Transactions on Information and System, 2003, **E86-D**(12): 2786-2789.

7　Chu S C, Roddick J F, Lu Z M, *et al*. Digital image watermarking method based on labeled bisecting clustering algorithm[J]. IEICE Transactions on Fundamentals, 2004, **E87-A**(1): 282-285

8　Tian Yuan, Cheng Yi-min, Wang Yi-xiao. A novel method of data hiding[J]. ACTA Electronica Sinica, 2004, **32**(9): 1444-1447. [田源, 程义民, 王以孝. 一种新的数据隐藏方法[J]. 电子学报, 2004, **32**(9): 1444-1447.]

9　Qiu Ying-qiang, Cheng Yi-min, Wang Yi-xiao. A VQ-based watermarking method for color image[J]. Journal of China University of Science and Technology, 2007, **37**(2): 135-142. [邱应强,程义民,王以孝. 一种基于矢量量化彩色图像的水印方法[J]. 中国科学技术大学学报, 2007, **37**(2): 135-142.]

10　Cheng Yi-min, Xie Yu-ming, Wang Yi-xiao, *et al*. A method for secret transmission of color video[J]. Journal of Image and Graphics, 2005, **10**(1): 93-97. [程义民, 谢于明, 王以孝等. 一种彩色视频信息的隐秘传输方法[J]. 中国图象图形学报, 2005, **10**(1): 93-97.]

11　Cheng Yi-min, Qian Zhen-xing, Wang Yi-xiao, *et al*. A method of information hiding based on the digital-position information[J]. Journal of Electronics & Information Technology, 2005, **27**(8): 1304-1309. [程义民,钱振兴,王以孝. 基于数位信息的信息隐藏方法[J]. 电子与信息学报, 2005, **27**(8): 1304-1309.]