基于数位信息的信息隐藏方法

程义民 钱振兴 王以孝 田 源
(中国科学技术大学电子科学与技术系 合肥 230026)

摘 要: 描述了一种基于数字位置信息的信息隐藏方法，给出了一个单位增广矩阵，并在此基础上给出了具体算法。该方法若用单个数位信息，在 $n=2^m-1$ 时，嵌入效率可达到 m，有较高的数据嵌入效率；若用多个数位组合信息，可在保持嵌入效率不变的条件下，数据嵌入率近似等于 1(n 较大时)，在相同比特数的宿主信息中，可嵌入较多的隐藏信息，可用于流媒体等信息量较大信息的隐藏。文中所述的方法，计算复杂度不高，易于硬件实现，已用微型计算机在局域网上进行了模拟实验，获得了较好的实验结果。

关键词: 单位增广矩阵， 流媒体， 嵌入效率， 嵌入率， “异或”运算
中图分类号: TP309 **文献标识码**: A **文章编号**: 1009-5896(2005)08-1304-06

A Method of Information Hiding Based on the Digital-Position Information

Cheng Yi-min Qian Zhen-xing Wang Yi-xiao Tian Yuan
(*Department of Electronic Science and Technology, UST of China, Hefei* 230026, *China*)

Abstract This paper presents a method of information hiding based on the digital-position information, bringing forward an augmented identity matrix and a definite arithmetic upon it. In this method, if the single digital-position information is used, embedding efficiency can achieve m when $n=2^m-1$. And if the multi-digital-position information is used, data embedding rate can almost reach 1 when n is big enough, with the condition of an unchanged embedding efficiency. So more information can be hided in the host information with same bits and it can be used in stream multimedia, hidings with great information, etc. The proposed method with low computing complexity can be realized easily. Satisfying experimental results are gained on PC and LAN.

Key words Augmented identity matrix, Stream multimedia, Embedding efficiency, Embedding rate, XOR operation

1 引言

随着数字多媒体技术及计算机网络的发展，多种媒体信息的存储、传输越来越方便，信息安全就引起了人们的重视。信息隐藏的研究，对于数字产品知识产权的保护[1]、机密多媒体信息的隐秘传输[2]等起了很大的作用。

信息隐藏研究主要分为两方面：一方面是对于将信息隐藏其中的宿主，主要研究将信息隐藏在哪些数据中，不易被检测到，或不易被人觉察，如以图像或语音信息作为宿主时，可将那些对人眼或人耳不敏感的数据位置，作为可修改矢量，使数据有较好的隐蔽性。另一方面是信息嵌入方法研究，既要有隐蔽性，又要有有效性，即要求对宿主可修改信息，改变越少越好；在相同宿主可修改比特中，嵌入数据越多越好。特别对语音等信息量大的流媒体，要有一定数据嵌入率，才能满足要求。但通常二者是矛盾的。

通常可用奇偶调制性，在 n bit 宿主可修改数据中，嵌入 n bit 需隐藏的数据，最多只要改变年 n bit 宿主数据，有较高的数据嵌入率，但对宿主数位改变较多，隐蔽性通常不是很好。

2002 年，Tseng 等人[3]给出了一种方法，最多只要修改 2bit，就可在 n bit 宿主可修改数据中嵌入 $\lfloor \log_2(n+1) \rfloor$ bit 需隐藏数据($\lfloor \bullet \rfloor$ 为向下取整运算)。2003 年 Galand 等人[4]给出了一种方案，在 n bit 宿主信息中，嵌入 $\lfloor \log_2(n+1) \rfloor$ bit 需隐藏数据，最多只需修改 1bit 信息。这些嵌入方法，有较好的隐蔽性。但当 $n=2^m-1$ 时，在(2^m-1)bit 宿主信息，只能嵌入 m bit 数据，数据嵌入率较低，常不能满足信息量大的多媒体信息隐藏的要求。

本文从一个较新的角度，描述了一种应用宿主可修改信息中数据数位信息的嵌入/提取方法。文中给出了一个单位增广矩阵，应用该单位增广矩阵的性质，通过“异或”运算来实现需隐藏数据到宿主可修改信息的嵌入及提取。

2004-03-02 收到，2004-11-08 改回

该方法对于单数位信息，在 n bit 宿主可修改信息，嵌入 $\lfloor \log_2(n+1) \rfloor$ bit 需隐藏数据，最多只需修改 1bit 宿主信息；若用多数位组合信息，可在保持嵌入效率不变的条件下，在 n bit 宿主可修改信息中，可嵌入 $(n-1)$ bit 需隐藏数据。n 较大时，数据嵌入率近似为 1，可满足一些流媒体等信息量较大的信息的隐藏。

文中所述方法，已用微型计算机在局域网上进行了模拟实验，获得了较好的结果。可在一帧 GSM 语音信息中，嵌入 20 ms 2.4 kb 语音数据，从而可以满足一路语音隐藏在另一路语音中通过公共无线信道隐藏传输的要求。

嵌入/提取算法，以一个二值单位增广矩阵及“异或”运算为基础，因此，计算复杂度不高，也易于用硬件实现。

2　单数位信息

如果 $\boldsymbol{a}=(a_1,a_2,\cdots,a_n)^{\mathrm{T}}$ 为二值可修改矢量，其单个数字位置信息可与 n 个数值对应，当 $n=2^m-1$ 时，则可与 $1,2,\cdots,(2^m-1)$，即 (2^m-1) 个 m bit 二进制数对应。

2.1 嵌入方法

若 $\boldsymbol{b}=(b_1,b_2,\cdots,b_m)^{\mathrm{T}}$ 为待隐藏的 m bit 二进制数码，$\boldsymbol{W}$ 为 $m\times n$ $(n=2^m-1)$ 的二值矩阵。如果 $\boldsymbol{W}$ 矩阵二值列矢量所对应的十进制数称为该列矢量的值，则 $\boldsymbol{W}$ 的列矢量 $\boldsymbol{w}_1,\boldsymbol{w}_2,\cdots,\boldsymbol{w}_n$ 的值可定义为一个从 1 到 (2^m-1) 的连续自然数数列。

令

$$\boldsymbol{c}=\boldsymbol{W}\boldsymbol{a}=\boldsymbol{w}_1a_1\oplus\boldsymbol{w}_2a_2\oplus\cdots\oplus\boldsymbol{w}_na_n \tag{1}$$

式(1)中，$\boldsymbol{c}$ 是 m 维矢量，为 $\boldsymbol{a}$ 中各数位的加权模二和，所以 $\boldsymbol{W}$ 矩阵可称为加权矩阵。

令

$$\boldsymbol{d}=\boldsymbol{b}\oplus\boldsymbol{c} \tag{2}$$

由于 $\boldsymbol{d}$ 为 m 维矢量，若为 $\boldsymbol{0}$ 矢量，则 $\boldsymbol{b}=\boldsymbol{c}$，$\boldsymbol{a}$ 不用作任何改变，$\boldsymbol{a}'=\boldsymbol{a}$。否则 $\boldsymbol{d}$ 的值一定在 $1\sim(2^m-1)$ 之间，这时一定可在 $\boldsymbol{W}$ 中找到一列，如 $\boldsymbol{w}_i=\boldsymbol{d}$，只要将 $\boldsymbol{a}$ 中对应的第 i 个元素取反

$$\boldsymbol{a}'=(a_1,\cdots,a_i\oplus1,\cdots,a_n) \tag{3}$$

这样，最多修改 1 位，便将 m bit 数据（$\boldsymbol{b}$）嵌入 n bit 数码。$\boldsymbol{a}'$ 为嵌入 $\boldsymbol{b}$ 后的可修改矢量。

2.2 提取方法

提取时，得到的是 $\boldsymbol{a}'$，由前面讨论知，当 $\boldsymbol{d}$ 值为 0 时，$\boldsymbol{a}'=\boldsymbol{a}$

则

$$\boldsymbol{W}\boldsymbol{a}'=\boldsymbol{w}_1a_1\oplus\boldsymbol{w}_2a_2\oplus\cdots\oplus\boldsymbol{w}_na_n=\boldsymbol{c}=\boldsymbol{b} \tag{4}$$

若 $\boldsymbol{d}$ 值不为 0 时，

$$\begin{aligned}\boldsymbol{W}\boldsymbol{a}'&=\boldsymbol{w}_1a_1\oplus\boldsymbol{w}_2a_2\oplus\cdots\oplus\boldsymbol{w}_i(a_i+1)\oplus\cdots\oplus\boldsymbol{w}_na_n\\&=\boldsymbol{w}_1a_1\oplus\boldsymbol{w}_2a_2\oplus\cdots\oplus\boldsymbol{w}_na_n\oplus\boldsymbol{w}_i=\boldsymbol{c}\oplus\boldsymbol{w}_i\end{aligned} \tag{5}$$

因为 $\boldsymbol{w}_i=\boldsymbol{d}$，所以

$$\boldsymbol{W}\boldsymbol{a}'=\boldsymbol{c}\oplus\boldsymbol{d}=\boldsymbol{c}\oplus\boldsymbol{b}\oplus\boldsymbol{c}=\boldsymbol{b} \tag{6}$$

因此，只需计算 $\boldsymbol{W}\boldsymbol{a}'$，就可得到嵌入的 m bit 信息 $\boldsymbol{b}$。

2.3 $\boldsymbol{W}$ 矩阵

当 $n=2^m-1$ 时，$\boldsymbol{W}$ 有(2^m-1)列，由 2.1 节知，数据嵌入时，只需在 $\boldsymbol{W}$ 中找到一列，如 $\boldsymbol{w}_i$，使得 $\boldsymbol{w}_i=\boldsymbol{d}$ 即可。所以 $\boldsymbol{W}$ 的列不一定非要按值从小到大的顺序排列，这样 $\boldsymbol{W}$ 矩阵就可有 $(2^m-1)!$ 种选择。

当 $n>2^m-1$ 时，若仍嵌入 m bit 信息，矩阵 $\boldsymbol{W}$ 中值为 $1\sim(2^m-1)$ 的列向量，每一列矢量只须出现一次即可，其它 $(n-2^m+1)$ 个列矢量值可为 $1\sim(2^m-1)$ 中的任一值。这样 $\boldsymbol{W}$ 矩阵就有 $C_n^{2^m-1}\cdot(2^m-1)!\cdot(2^m-1)^{n-2^m+1}$ 种选择。当 n 较大时，这是一个非常大的数，所以 $\boldsymbol{W}$ 矩阵也可作为一种密钥使用。

对与上述每一不同 $\boldsymbol{W}$ 矩阵，上述嵌入算法只需稍许改动即可，提取方法基本不变。

3　多数位组合信息

如果选择 L 位信息，$1<L<n$，对于二值可修改矢量 $\boldsymbol{a}=(a_1,a_2,\cdots,a_n)^{\mathrm{T}}$，有 $C_n^0+C_n^1+C_n^2+\cdots+C_n^L$ 个数位信息，可有相应多个数值与其对应。若要嵌入 m bit 数据，则需满足：

$$2^m\le C_n^0+C_n^1+C_n^2+\cdots+C_n^L \tag{7}$$

由排列与组合的理论可知[5]：对于 C_n^k，当 n 为偶数时，在 $k=n/2$ 处有最大值；当 n 为奇数时，在 $k=(n-1)/2$ 或 $k=(n+1)/2$ 处有最大值。所以取 $n=2L+1$ 时，可在修改较少比特条件下，嵌入较多数据。

由二项展开式知：

$$(1+x)^n=C_n^0x^n+C_n^1x^{n-1}+\cdots+C_n^nx^0,\quad x\le1 \tag{8}$$

令 $x=1$，有 $2^n=C_n^0+C_n^1+\cdots+C_n^n$。令 $n=2L+1$，

$$2^{2L+1}=C_{2L+1}^0+C_{2L+1}^1+\cdots+C_{2L+1}^{2L+1} \tag{9}$$

因为 $C_{2L+1}^k=C_{2L+1}^{2L+1-k}$，所以 $2^{2L+1}=2(C_{2L+1}^0+C_{2L+1}^1+\cdots+C_{2L+1}^L)$

$$2^{2L}=C_{2L+1}^0+C_{2L+1}^1+\cdots+C_{2L+1}^L \tag{10}$$

与式(7)相比较可知，当 $n=2L+1$，$m=2L$ 时，式(7)为一等式，即当 n 为 $2L+1$ 时，对于 L 个数位组合信息，恰可与 2^{2L} 个数字对应。

由 2.1 节嵌入方法知，需在 $\boldsymbol{W}$ 矩阵中找到与 $\boldsymbol{d}$ 相同的 $\boldsymbol{w}_i$，才能将相应数据 $\boldsymbol{b}$ 嵌入到可修改矢量 $\boldsymbol{a}$ 中。由于 $2^{2L}>2L+1(L\ge1)$，不可能对每一 $2L$ bit 数，找到与其值

相等的列矢量，但是，只要找到不多于 L 个列矢量，如 $\boldsymbol{w}_{i1}$，$\boldsymbol{w}_{i2}$，…，$\boldsymbol{w}_{ik}$，$k\le L$，对任一 $1\sim(2^{2L}-1)$ 整数对应的二值矢量 $\boldsymbol{d}$ 有：

$$\boldsymbol{d}=\boldsymbol{w}_{i1}\oplus\boldsymbol{w}_{i2}\oplus\cdots\oplus\boldsymbol{w}_{ik} \tag{11}$$

则上述算法仍然成立。满足式(11)的加权矩阵可称为 $\boldsymbol{W}^{(L)}$ 矩阵，在该矩阵中，任一 $1\sim(2^{2L}-1)$ 中的整数对应的 $2L$ 维矢量，都最多可由 $\boldsymbol{W}^{(L)}$ 中不超过 L 个列矢量，通过“异或”运算产生。

3.1 二值单位增广矩阵

对任一 n 阶单位矩阵，再增加一列全“1”二值列矢量作为第 $(n+1)$ 列，可得到一个 $n\times(n+1)$ 二值单位增广矩阵，可称为 n 阶二值单位增广矩阵，其第1列到第 $(n+1)$ 列的值为一数列：2^{n-1}，$2^{n-2},\cdots,2^0$，2^n-1。

3.1.1 四阶二值单位增广矩阵　式(12)给出了一个四阶单位增广矩阵。

$$\begin{bmatrix}1&0&0&0&1\\0&1&0&0&1\\0&0&1&0&1\\0&0&0&1&1\end{bmatrix}_{4\times5} \tag{12}$$

由式(12)可知，对任一 $1\sim2^4-1=15$ 的整数所对应的四维矢量 $\boldsymbol{d}$，都可在四阶二值单位增广矩阵中找到不超过两个列矢量，如 $\boldsymbol{w}_{i1},\cdots,\boldsymbol{w}_{ik}\,(k\le2)$，使得

$$\boldsymbol{d}=\boldsymbol{w}_{i1}\oplus\cdots\oplus\boldsymbol{w}_{ik} \tag{13}$$

式(12)的四阶单位增广矩阵，满足式(11)条件，可称为 $\boldsymbol{W}^{(2)}$ 矩阵。

3.1.2 $2L$ 阶二值单位增广矩阵　式(14)给出了一个 $2L$ 阶单位增广矩阵，其第1列到 $(2L+1)$ 列列矢量的值为数列：$2^{2L-1},2^{2L-2},\cdots,2^1,2^0,2^{2L}-1$。

$$\begin{bmatrix}1&0&0&\cdots&0&0&1\\0&1&0&\cdots&0&0&1\\0&0&1&\cdots&0&0&1\\\vdots&\vdots&\vdots&\ddots&\vdots&\vdots&\vdots\\0&0&0&\cdots&1&0&1\\0&0&0&\cdots&0&1&1\end{bmatrix}_{2L\times(2L+1)} \tag{14}$$

对于任一值为 $1\sim(2^{2L}-1)$ 的 $2L$ 维二值矢量 $\boldsymbol{d}$，

$$\boldsymbol{d}=(d_1,d_2,\cdots,d_{2L})^{\mathrm{T}}=\begin{bmatrix}d_1\\d_2\\\vdots\\d_{2L}\end{bmatrix}$$

(1) 如果 $\boldsymbol{d}$ 中 1 的个数 k 介于1与 L 之间，即 $1\le k\le L$，如 $\boldsymbol{d}$ 中 $d_{i1},d_{i2},\cdots,d_{ik}$ 值为“1”，其余值为“0”。由于式(14)中前 $2L$ 列为一单位阵，每一列有且只有一个“1”，所以对 $\boldsymbol{d}$ 中每一值为“1”的行，如 d_{ik}，在式(14)前 $2L$ 列的单位阵中都可以找到且只能找到一个相应行值为“1”的列 $\boldsymbol{w}_{ik}$，共可找到 k 列 $(1\le k\le L)$，使得

$$\boldsymbol{d}=\boldsymbol{w}_{i1}\oplus\boldsymbol{w}_{i2}\oplus\cdots\oplus\boldsymbol{w}_{ik} \tag{15}$$

(2)如果 $\boldsymbol{d}$ 中 1 的个数 k，介于 L 和 $2L$ 之间，即 $L<k\le2L$，则其中零的个数 J 介于 $L-1$ 到 0 之间，即 $0\le J\le L-1$。如 $\boldsymbol{d}$ 中 d_{i1},d_{i2},L,d_{iJ} 值为“0”，其余值为“1”，则对值为“0”的行，可在式(14)前 $2L$ 列中，找到且只能找到相应行值为“1”的列，共 J 列，$0\le J\le L-1$，再加上第 $2L+1$ 全“1”列，总共不超过 L 列，使

$$\boldsymbol{d}=\boldsymbol{w}_{i1}\oplus\boldsymbol{w}_{i2}\oplus\cdots\oplus\boldsymbol{w}_{iJ}\oplus\boldsymbol{w}_{2L+1} \tag{16}$$

因此，对任一非零 $2L$ 阶二值矢量 $\boldsymbol{d}$，都可在矩阵式(14)中找到不超过 L 列 $\boldsymbol{w}_{i1},\boldsymbol{w}_{i2},\cdots,\boldsymbol{w}_{ik}$，$(1\le k\le L)$使

$$\boldsymbol{d}=\boldsymbol{w}_{i1}\oplus\boldsymbol{w}_{i2}\oplus\cdots\oplus\boldsymbol{w}_{ik} \tag{17}$$

式(14)的 $2L$ 阶二值单位增广矩阵也满足上述式(11)条件，可称其为 $\boldsymbol{W}^{(L)}$ 矩阵。

3.2 嵌入/提取方法

3.2.1 嵌入方法　若 $\boldsymbol{a}=(a_1,a_2,\cdots,a_{2L+1})$ 为可修改矢量，$\boldsymbol{b}=(b_1,b_2,\cdots,b_{2L})$ 为待嵌入数据，$\boldsymbol{W}^{(L)}$ 矩阵为如式(14)的 $2L$ 阶二值单位增广矩阵，计算

$$\boldsymbol{c}=\boldsymbol{W}^{(L)}\boldsymbol{a}=\boldsymbol{w}_1^{(L)}a_1\oplus\boldsymbol{w}_2^{(L)}a_2\cdots\oplus\boldsymbol{w}_{2L+1}^{(L)}a_{2L+1} \tag{18}$$

其中 $\boldsymbol{c}$ 为 $2L$ 维二值矢量。令

$$\boldsymbol{d}=\boldsymbol{b}\oplus\boldsymbol{c} \tag{19}$$

$\boldsymbol{d}$ 也为一 $2L$ 维矢量，若 $\boldsymbol{d}$ 值为零，则 $\boldsymbol{b}=\boldsymbol{c}$，$\boldsymbol{a}$ 不作任何变化；若 $\boldsymbol{d}$ 不为零，由 3.1.2 节可知，可在 $2L$ 阶二值单位增广矩阵中，找到不超过 L 列，使得

$$\boldsymbol{d}=\boldsymbol{w}_{i1}\oplus\boldsymbol{w}_{i2}\oplus\cdots\oplus\boldsymbol{w}_{ik},\quad 1\le k\le L \tag{20}$$

与2.1节类似，只需将 $\boldsymbol{a}$ 中与式(20)中列向量对应的不超过 L 个元素取反，即

$$\boldsymbol{a}'=(a_1,\cdots,a_{i1}\oplus1,\cdots,a_{i2}\oplus1,\cdots,a_{ik}\oplus1,\cdots,a_{2L+1}) \tag{21}$$

这样最多修改 L bit 就可将 $2L$ bit 数据嵌入 $(2L+1)$bit 宿主可修改信息中。

3.2.2 提取方法　提取方法与 2.2 节类似，当 $\boldsymbol{d}$ 为零时，$\boldsymbol{b}=\boldsymbol{c}$，所以

$$\boldsymbol{W}^{(L)}\boldsymbol{a}'=\boldsymbol{W}^{(L)}\boldsymbol{a}=\boldsymbol{w}_1^{(L)}a_1\oplus\boldsymbol{w}_2^{(L)}a_2\cdots\oplus\boldsymbol{w}_{2L+1}^{(L)}a_{2L+1}=\boldsymbol{c}=\boldsymbol{b} \tag{22}$$

当 $\boldsymbol{d}$ 不为零时，

$$\begin{aligned}\boldsymbol{W}^{(L)}\boldsymbol{a}'=&\boldsymbol{w}_{2L+1}^{(L)}a_1\oplus\cdots\oplus\{\boldsymbol{w}_{i1}^{(L)}(a_{i1}\oplus1)\}\oplus\cdots\\&\oplus\{\boldsymbol{w}_{i2}^{(L)}(a_{i2}\oplus1)\}\oplus\cdots\oplus\{\boldsymbol{w}_{ik}^{(L)}(a_{ik}\oplus1)\}\\&\oplus\cdots\oplus\boldsymbol{w}_{2L+1}^{(L)}a_{2L+1}\\=&\boldsymbol{w}_1^{(L)}a_1\oplus\boldsymbol{w}_2^{(L)}a_2\oplus\cdots\oplus\boldsymbol{w}_{2L+1}^{(L)}a_{2L+1}\\&\oplus\boldsymbol{w}_{i1}^{(L)}\oplus\boldsymbol{w}_{i2}^{(L)}\oplus\cdots\oplus\boldsymbol{w}_{ik}^{(L)}\end{aligned} \tag{23}$$

由式(18)、式(19)和式(20)知，这时，

$$\boldsymbol{W}^{(L)}\boldsymbol{a}'=\boldsymbol{c}\oplus\boldsymbol{d}=\boldsymbol{c}\oplus\boldsymbol{b}\oplus\boldsymbol{c}=\boldsymbol{b} \tag{24}$$

3.2.3 $W^{(L)}$ 矩阵　上面讨论 $n=2L+1$ 时情况，3.2.1 节嵌入算法中，只要找到不超过 L 个列，使式(20)成立即可，与列的排序无关，所以此时 $W^{(L)}$ 矩阵有 $(2L+1)!$ 种选择。

当 $n>2L+1$ 时，若仍嵌入 $2L$ bit 数据，$1\sim(2^{2L}-1)$ 的每一数所对应的 $2L$ 维列矢量，至少要出现一次，其余 $(n-2L-1)$列可为前面任一列矢量，所以此时 $W^{(L)}$ 矩阵可有 $(2L+1)!\cdot C_n^{2L+1}\cdot(2L+1)^{n-2L-1}$ 种选择，当 n 较大时，这是一个很大的数，可作为密钥使用。

4　嵌入效率及嵌入率

若将改变每 1 bit 宿主所嵌入的比特数称为嵌入效率 η，则用单数位信息，最多只需改变 1 bit 宿主信息。由 2.1 节知，此时，最小嵌入效率为

$$\eta=\lfloor\log_2(n+1)\rfloor \tag{25}$$

其中 $\lfloor\bullet\rfloor$ 为下取整，n 为可修改矢量的长度，当 $n=2^m-1$ 时，$\eta=m$。

用多数位组合信息时，最多只需改变 L bit，由 3.2.1 知，此时，

$$\eta=2L/L=2 \tag{26}$$

即嵌入效率为一常数 2，而与可修改矢量的长度无关。

通常，嵌入效率越高，嵌入同样信息时，对宿主信息改变越小，隐蔽性越好。

若将宿主可修改矢量中，平均每 1 bit 可以嵌入的比特数称为数据嵌入率 α，则对于用单数位信息，由 2.1 节知

$$\alpha=\log_2(n+1)/n \tag{27}$$

当 $n=2^m-1$ 时，

$$\alpha=m/(2^m-1) \tag{28}$$

其中 n 为可修改的矢量长度，当 m 较大时，数据嵌入率则较小。

用多数位组合信息时，由 3.2.1 知，

$$\alpha=2L/(2L+1) \tag{29}$$

当 $n=2L+1$ 时，

$$\alpha=(n-1)/n \tag{30}$$

因此，应用单数位信息，有较高的嵌入效率，但数据嵌入率较低，即相同长度可修改信息，可嵌入的数据较少，特别是 m 较大时，α 就很小。用多数位组合信息时，嵌入效率为一常数 2，而嵌入率小于接近于 1，特别是 n 较大时，$\alpha\approx1$。

5　实验及结果

为了验证文中所述方法，我们在计算机和局域网中进行了模拟，所用 IP 终端为 PIII 微型计算机，软件平台为 Windows 2000。下面给出部分实验结果。

5.1 彩色图像的隐藏实验

这一组实验，主要验证 2.1 节，2.2 节所述方法的正确性，模拟过程是将一幅彩色图像隐藏在作为宿主的视频段，经局域网传输后，在接收端提取出隐藏的彩色图像。

实验所用视频一些是从娱乐视频中截取的 MPEG-2 格式的视频段，一些是从官方网站下载的 MPEG-2 标准视频。这些视频经部分解压，取其每一字块 DCT 对人眼不敏感的中频段值大于 T 的系数的最低位，作为可修改矢量，用 2.1 节，2.2 节的嵌入/提取方法。数据嵌入时，每一子块只有 1 bit 数据被修改。

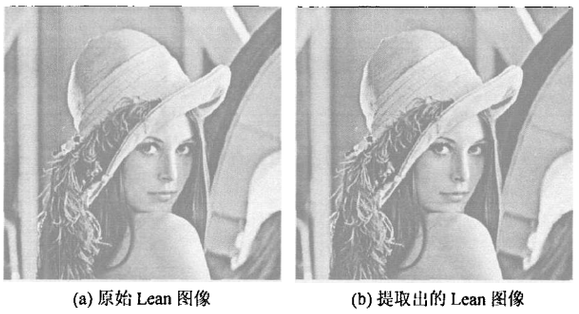
图 1 给出了在视频段 1 中隐藏 Lena 彩色图像的实验结果。视频段 1 每帧大小为 720×480，共 177 帧，其中图 1(a)是未隐藏信息时 3 帧原始视频图像，图 1(b)是隐藏信息后相应的视频帧。由图 1 可知，该嵌入方法有着较好的视觉效果。图 2(a)是隐藏的原始 Lena 图像，图 2(b)是提取出的 Lena 图像。(实验中使用的视频和图像均为彩色，为印刷方便，这里给出的是相应的灰度图像，下同)。

表 1 给出了一组实验的统计结果。从实验结果可看出，该方法具有较高的平均 PSNR。实验没有考虑噪声及远距离传输对数据的影响，其正确提取率均为 100%，未在表中列出。

(a) 原始视频图像帧

(b) 隐藏有彩色图像的相位视频图像帧

图 1　原始视频帧和隐藏数据后视频帧的比较



(a) 原始 Lean 图像　　(b) 提取出的 Lean 图像

图 2

表 1 不同视频隐藏图像实验相关数据

视 频	视频帧数	嵌入数据大小(bit)	平均数据嵌入码率(kbit/s)	原视频大小(Mb)	嵌入数据后视频大小(Mb)	平均 PSNR(dB)
视频段 1	177	560392	95.0	2.66	2.69	46.17
视频段 2	735	1739280	80.0	10.0	9.97	45.16
视频段 3	325	1669880	154.1	6.87	6.93	44.42
视频段 4	344	1442952	125.8	5.87	5.93	46.99
Cact_040(4.0Mbit/s)	450	1623620	108.2	7.17	7.24	40.27
Cact_080(8Mbit/s)	450	4084070	272.3	14.3	14.4	41.05
Susi_040(4.0Mbit/s)	450	1779062	118.6	7.16	7.23	44.75
Susi_080(8Mbit/s)	450	4240152	282.7	14.3	14.4	43.77

5.2 语音信息的隐藏实验

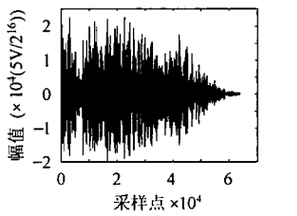
这一组实验主要验证 3.2 节所述方法的正确性，实验过程是将一路 2.4kb/s MELP 语音，隐藏在另一路 GSM 编码的语音中，经局域网实时传输，在接收端再将 2.4kb/s MELP 语音信息提取出来，从而模拟语音信号的隐秘传输。

实验软件平台为 Windows2000, 采集的音频信号为 16 bit 线性 PCM 音频信号，采样时间为 8s，共 64000 个样点。采用 GSM 编码，由 ITU 对 GSM 编码重要性分类[6]中，每帧对人耳不敏感的 69bit 中，选取 49bit 作为宿主可修改矢量，用 3.2 节方法，最多修改 24bit，相应嵌入 48 bit 的 MELP 编码的 20ms 语音信息。图 3 给出了一组宿主语音的实验结果，图 4 给出了所嵌入的 MELP 语音的实验结果。其中横轴是样点个数，纵轴是幅值(单位为 $(5V/2^{16})$)。

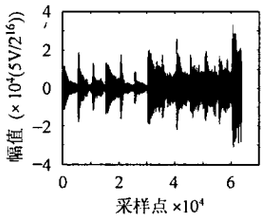
实验表明，在 GSM 编码语音中可嵌入一路 2.4kb/s 的 MELP 编码的隐秘语音，嵌入后对宿主语音信号的信噪比影响较小，具有较好的音频质量。人耳基本不能分辨出嵌入前后 GSM 语音的区别。嵌入的 2.4kb/s MELP 编码的隐秘语音在局域网模拟实验可实现 100%的正确提取率。表 2 给出了 10 组实验的统计结果，实验中传输的 MELP 编码语音的正确提取率为 100%。

表 2 不同信噪比语音信号实验数据

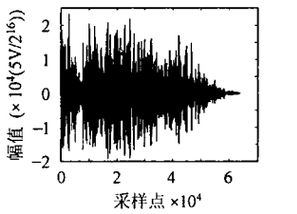
原始 PCM 语音信噪比(dB)	共嵌入数据大小(bit)	平均数据嵌入码率(bit/s)	GSM 语音编码解码后信噪比 SNR(dB)	语音经 GSM 编码嵌入 MELP 语音解码后平均信噪比 SNR(dB)
23.1	19200	2400	22.4	22.3
44.3	19200	2400	43.3	43.2
48.5	19200	2400	47.8	48.0
48.2	19200	2400	47.2	46.8
50.9	19200	2400	50.1	50.2
35.9	19200	2400	34.9	35.3
46.7	19200	2400	46.1	45.9
37.0	19200	2400	36.3	36.0
31.8	19200	2400	30.9	31.2
38.6	19200	2400	37.8	37.8



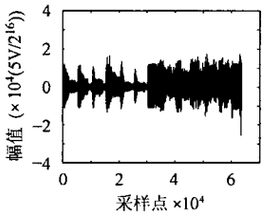
(a) 原始语音 (PCM) 平均信噪比 SNR=46.7dB



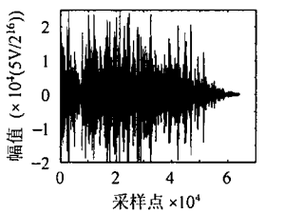
(a) 原始隐秘语音 (PCM)



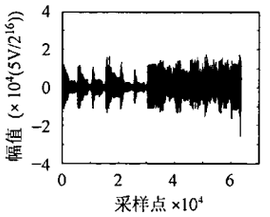
(b) 原始语音经 GSM 编码传输后解码 (PCM)，平均信噪比 SNR=46.1dB



(b) 隐秘语音经 MELP 编码后直接解码恢复的 PCM 语音



(c) 原始语音经 GSM 编码，嵌入 19200bit MELP 传输后解码 (PCM)，平均信噪比 SNR=45.9dB



(c) 隐秘语音经 MELP 编码后嵌入 GSM 语音中，传输后经提取解码恢复的 PCM 语音

图 3　　图 4

5　结束语

信息隐藏常在作为宿主的多媒体信息中，提取对人眼(耳)不敏感，或不易被检测到变化的信息，作为可修改信息，通过嵌入算法可将需隐藏的信息，隐藏到宿主信息中，人眼(耳)不易觉察或不易被侦测到的部位。

本文讨论了将宿主可修改信息用矢量表示，利用其数据位置信息嵌入需隐藏数据的方法，给出了两种二值加权矩阵，及数据嵌入/提取的具体算法，加权矩阵常可作为密钥使用。

若用单个数据位信息，其加权二值矩阵可以是一个列向量值为连续自然数列的矩阵。用该方法可在 n bit 可修改宿主信息中嵌入 $\lfloor \log_2(n+1) \rfloor$ bit 需隐藏数据，最多只需修改 1 bit 宿主信息，有较高的数据嵌入效率。若用多数位组合信息，其加权矩阵可为一单位增广矩阵。用该方法，可在 $(2L+1)$ bit 可修改宿主信息中嵌入 $2L$ bit 需隐藏数据，最多只需修改 L bit 宿主信息。在数据嵌入效率不变的的条件下，n 较大时，数据嵌入率近似为 1，有较高的数据嵌入率，可满足一些流媒体及数据量较大信息的隐藏。

所述方法已经在计算机局域网进行了模拟，获得了较好的结果。已成功的将 20ms 2.4kb 语音信息隐藏到 20ms GSM 编码语音的非敏感数据中，并通过了模拟实验，该方法能满足这些语音信息实时传输要求。该方法主要用二值加权矩阵及“异或”运算实现，因此计算复杂度不高且易于硬件实现。

文中主要讨论信息隐藏/提取算法，噪声及其它因素对隐藏信息的影响尚需进一步研究。

参 考 文 献

[1] Suhail M A, Obaidat M S. Digital watermarking-based DCT and JPEG model. *IEEE Trans. on Instrumentation and Measurement*, 2003, 52(5): 1640 – 1647.

[2] 陆红琳, 程义民, 王以孝, 田源. 一种基于 ICA 的汉字信息隐秘传输方法[J]. 中文信息学报, 2003, 17(4): 59 – 65.

[3] Tseng Yu-Chee, Chen Yu-Yuan, Pan Hsiang-Kuang. A secure data hiding scheme for binary images[J]. *IEEE Trans. on Communications*, 2002, 50(8): 1227 – 1231.

[4] Galand F, Kabatiansky G. Information hiding by coverings. Information Theory Workshop, Paris, France, 2003, IEEE, 2003: 151 – 154.

[5] 吴世煦. 排列与组合. 江苏:江苏人民教育出版社, 1979: 62.

[6] Digital cellular telecommunications systems (phase2+), Full rate speech, Transcoding[J]. GSM 06.10 Version 7.0.2 Release, 1998: 58 – 59.

程义民：　男，1945 年生，教授，博士生导师，研究领域为信息隐藏、网络多媒体、计算机视觉、深度图像分析等.

钱振兴：　男，1981 年生，硕博连读研究生，研究领域为信息隐藏、图象处理、网络多媒体等.

王以孝：　男，1946 年生，副教授，研究领域为信息隐藏、视频图像传输及通信技术、深度图像分析等.