

# 一种彩色视频信息的隐秘传输方法

程义民 谢于明 王以孝 郭志川

(中国科学技术大学 电子科学与技术系, 计算机视觉实验室, 合肥 230026)

**摘要** 为了实现数据量较大的流媒体彩色视频信息的隐秘传输, 描述了一种将 low level MPEG-II 彩色视频信号隐藏在另一路 main level MPEG-II 彩色视频中, 并通过公共信道进行传输的方法。该方法利用人眼视觉特性, 在宿主视频图像的 DCT 域, 选择对人眼不敏感的中高频信息作为宿主可修改矢量, 并提出了一个新的数据嵌入方法, 由于该方法最多修改  $L$  bits 宿主信息, 就可在  $(2L+1)$  bits 宿主可修改矢量中嵌入  $2L$  bits 信息, 因此有较高的数据嵌入率及较好隐蔽性。该方法也可用于其他流媒体及较大信息量信息的隐秘传输。该方法已在局域网上进行了模拟, 并获得了较好的结果。

**关键词** MPEG-II 嵌入/提取 流媒体 数据嵌入率

**中图分类号:** TN918.74 **文献标识码:** A **文章编号:** 1006-8961(2005)01-0093-05

## A Method for Secret Transmission of Color Video

CHENG Yi-min, XIE Yu-ming, WANG Yi-xiao, GUO Zhi-chuan

(Laboratory of Computer Vision, Department of Electronic Science & Technology, University of Science & Technology of China, Hefei 230026)

**Abstract** In order to realize secret transmission of great color video information. This paper presents a new scheme capable of hiding low level MPEG-II color video streams into main level MPEG-II color video streams. It makes full use of vision character of our eyes and selects information of intermediate/high frequency as revisable host vector in the DCT domain of host video streams, which are not sensitive to our eyes. A novel embedding method is proposed in this paper. As many as  $2L$  bits of information data can be embedded by changing, at most,  $L$  bits in the  $(2L+1)$  bits cover data, which makes higher data-embedding efficiency and better secrecy. The scheme can be also used for secret transmission of other stream media and great information. The scheme has been simulated in Local area Networks and better experimental results have been given.

**Keywords** MPEG-II, embedding/extracting, stream media, data embedding rate

## 1 引言

信息隐藏是信息处理领域的重要研究课题之一, 可广泛应用于知识产权保护<sup>[1]</sup>、信息的隐秘传输<sup>[2]</sup>等, 但在该研究领域, 被隐藏的信息量大小与其隐蔽性的矛盾常较难解决。彩色视频, 因其信息量大, 又要实时隐秘传输, 使这一矛盾更为突出。

为了增加隐蔽性, 则常需对宿主信息进行分析研究, 通过寻找那些对人眼、耳不敏感, 或不易被检测到变化的信息来作为宿主可修改矢量; 另一方面,

在宿主可修改矢量一定的条件下, 研究有效的数据嵌入方法, 而且要求对宿主信息修改越少, 嵌入数据越多, 才表明方法越好。

2002年 Yu-Chen Tseng 等人给出了一种方法<sup>[3]</sup>, 最多只要修改 2bits, 就可在  $n$  bits 宿主可修改矢量中嵌入  $[\log_2(n+1)]$  bits 数据。2003年 Galand 等人给出了在相同条件下, 嵌入  $[\log_2(n+1)]$  bits 数据, 而最多只需修改 1 bit 的方案<sup>[4]</sup>。这些方法, 当嵌入  $m$  bits 数据时, 则可修改矢量达  $(2^m - 1)$  bits, 当  $m$  较大时, 这是一个较大的数, 由于其数据嵌入率较低, 因此常不能满足彩色视频等流媒体及较大信息

收稿日期: 2004-03-22; 改回日期: 2004-07-23

**第一作者简介:** 程义民(1945 ~ ), 男, 1969年毕业于中国科学技术大学无线电系计算机专业, 1984 ~ 1985年, 在英国 Hull 大学作访问研究员, 现为中国科学技术大学电子科学与技术系教授, 博士生导师。主要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。  
E-mail: ymcheng@ustc.edu.cn

量信息隐藏及隐秘传输的需要。

奇偶调制法<sup>[5]</sup>是一种数据嵌入率较高的方法,其可在  $n$  bits 宿主可修改矢量中,嵌入  $n$  bits 数据,但由于该方法最多需修改  $n$  bits 宿主信息,因而不利于被隐藏信息的隐蔽。

为此文中提出了一种新的数据嵌入方法,该方法可在  $(2L+1)$ bits 宿主可修改矢量中,嵌入  $2L$  bits 数据,且最多只需修改  $L$  bits 宿主信息,由于它不仅具有较高数据嵌入率,且对宿主信息修改也较少,因而较适用于流媒体及信息量较大信息的隐藏及隐秘传输。

本文给出了一个方案,即利用人眼视觉特性及新的嵌入方法,较好地解决了视频待隐藏数据量较大及隐蔽性的矛盾,并在局域网上,成功实现了将一路 low level MPEG-II 彩色视频信号隐藏在另一路 main level MPEG-II 彩色视频中的实时隐秘传输模拟实验。

## 2 系统概述

图1给出了将一路 low level MPEG-II 彩色视频图像隐藏在另一路 main level MPEG-II 彩色视频图像中的隐秘传输发送端框图。

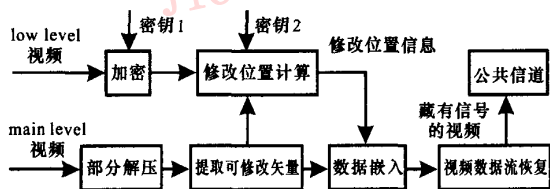


图1 发送端框图

Fig. 1 Block diagram of a transmitter

main level MPEG-II 彩色视频,经过部分解压后即得到每  $8 \times 8$  子块的 DCT (discrete cosine transform) 系数数值,再根据人的视觉特性,通过选其对人眼不敏感的中高频部分 DCT 系数,取其最低位来组成宿主可修改矢量。

待隐秘传输的 low level MPEG-II 彩色视频信号,其经加密后的数据流,在分组形成待嵌入数据矢量,再结合宿主可修改矢量及密钥2计算嵌入当前组数据时,需修改宿主的位置信息。

按得到的需修改的宿主位置信息,先修改相应 DCT 系数的数据位(取反),再经行程编码、Huffman 编码等进行恢复,即得到藏有 low level MPEG-II 视频数据的 main level MPEG-II 视频流,然后就可按通

常方式通过公共信道传输。

在接收端,将接收到藏有数据的 main level MPEG-II 视频,经过部分解压后,先按第4节提取方法,即可得到被隐藏的一路 low level MPEG-II 视频信息,然后再经解密,即可通过公共信道实现一路 low level MPEG-II 彩色视频隐藏在另一路 main level MPEG-II 彩色视频中的隐秘传输,而且对原宿主 main level MPEG-II 彩色视频信息的影响则很难觉察。

该方法也可用于其他流媒体信息的隐秘传输。

## 3 单位增广矩阵

在一个  $n$  阶单位矩阵中,增加一个全“1”列矢量,即组成一个  $n$  阶二值单位增广矩阵。若将各列矢量相应的十进制数列出,则自第1列至第  $(n+1)$  列的值依次为  $2^{n-1}, 2^{n-2}, \dots, 2^1, 2^0, 2^n - 1$ 。其前  $n$  个值分别为  $n$  位二进制数各数位的权值,这  $n$  列不妨称为权值列,而最后一列则为  $n$  位二进制数的最大值。

### 3.1 4 阶单位增广矩阵

式(1)给出了一个4阶单位增广矩阵,即

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix}_{4 \times 5} \quad (1)$$

与其列矢量对应的十进制数依次为 8, 4, 2, 1, 15。

由式(1)可见:对  $1 \sim (2^4 - 1)$  的十进制数中与任一值对应的二值矢量,均可由4阶单位增广矩阵中不超过2个列矢量的异或运算获得。

### 3.2 $2L$ 阶单位增广矩阵

式(2)为一  $2L$  阶单位增广矩阵,即

$$\mathbf{W}_{2L \times (2L+1)} = \begin{bmatrix} 1 & 0 & 0 & \dots & 0 & 1 \\ 0 & 1 & 0 & \dots & 0 & 1 \\ 0 & 0 & 1 & \dots & 0 & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 1 \end{bmatrix}_{2L \times (2L+1)} \quad (2)$$

对于任一  $1 \sim (2^{2L} - 1)$  十进整数,其所对应的  $2L$  维二值列矢量  $\mathbf{d}$ ,具有以下特征:

(1) 若  $\mathbf{d}$  中“1”的个数为  $k, 1 \leq k \leq L$ ,则可在  $2L$  阶单位增广矩阵的由前  $2L$  列组成的  $2L$  阶单位阵中,由与这  $k$  个“1”所在行对应的权值列,通过异或

运算来得到这一列矢量  $d$ 。

(2)若  $d$  中的“1”的个数大于  $L$ , 即  $L < k \leq 2L$ , 则  $d$  中“0”的个数为  $j = 2L - k$ , 所以  $0 \leq j \leq L - 1$ , 此时, 可在  $2L$  单位阵中, 由这  $j$  个“0”所在行对应的权值列, 连同全“1”列通过异或运算即可得到列矢量  $d$ 。

由此可见, 对于  $1 \sim (2^{2L} - 1)$  的十进整数中与任一值对应的  $2L$  维二值列矢量  $d$ , 均可在  $2L$  阶单位增广矩阵中, 找到不超过  $L$  个列矢量, 满足

$$d = w_{i_1} \oplus w_{i_2} \oplus \dots \oplus w_{i_k} \quad (1 \leq k \leq L)$$

这里  $w_{i_1}, w_{i_2}, \dots, w_{i_k}$  为  $2L$  单位增广矩阵  $W_{2L \times (2L+1)}$  中满足上述条件的列矢量。

### 4 嵌入/提取方法

设  $f = (f_1, f_2, \dots, f_n)$  为  $n$  bits 的宿主数据矢量,  $g = (g_1, g_2, \dots, g_n)$  为信息数据嵌入后生成的数据矢量,  $c = (c_1, c_2, \dots, c_m)$  为待嵌入信息数据矢量,  $W_{m \times n}$  为一单位增广矩阵。

#### 4.1 $m = 2L, n = 2L + 1$ 时, 隐秘信息的嵌入/提取

$$s^T = W_{2L \times (2L+1)} f^T = \begin{bmatrix} 1 & 0 & 0 & \dots & 0 & 1 \\ 0 & 1 & 0 & \dots & 0 & 1 \\ 0 & 0 & 1 & \dots & 0 & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 1 \end{bmatrix}_{2L \times (2L+1)} \times$$

$$\begin{bmatrix} f_1 \\ f_2 \\ \vdots \\ f_{2L+1} \end{bmatrix} = \sum_{i=1}^{2L+1} f_i W_i \quad (3)$$

其中,  $W_i$  为  $W_{2L \times (2L+1)}$  矩阵中的第  $i$  列, “T” 表示矩阵的转置运算, “ $\sum$ ” 表示进行异或运算。从式 (3) 可得到  $s$  为  $2L$  维行矢量。

若对任意给出的  $m = 2L$  维待嵌入信息行矢量  $c = (c_1, c_2, \dots, c_{2L})$  与  $2L$  维行矢量  $s$  进行异或运算, 则可得到以下  $2L$  维行矢量

$$d^T = c \oplus s \quad (4)$$

若  $d = 0$  时, 即  $c = s$ , 则不需对宿主矢量  $f$  进行修改, 即  $g = f$ 。

若  $d \neq 0$  时, 由 3.2 节知, 可从矩阵  $W_{2L \times (2L+1)}$  中的  $(2L + 1)$  个列矢量中选  $1 \leq k \leq L$  个列矢量进行异或运算, 使  $d = w_{i_1} \oplus w_{i_2} \oplus \dots \oplus w_{i_k}$  ( $w_{i_1}, w_{i_2}, \dots, w_{i_k}$  分别为从矩阵  $W$  中选出的  $k$  列矢量)。若将宿主行矢

量  $f$  的相对应  $i \in (i_1, i_2, \dots, i_k)$  位取反, 则可得到嵌入信息后的矢量  $g$ , 即

$$g_i = \begin{cases} f_i & i \notin (i_1, i_2, \dots, i_k) \\ 1 \oplus f_i & i \in (i_1, i_2, \dots, i_k) \end{cases} \quad (5)$$

提取时, 只需计算  $Wg^T$  即可, 计算  $Wg^T$  时,

若  $d = 0$  时,

因为  $g = f, c = s$ ,

所以  $Wg^T = Wf^T = s^T = c^T$

若  $d \neq 0$  时,

$$\begin{aligned} Wg^T &= \sum_{i=1}^{2L+1} g_i w_i \\ &= \sum_{i \notin (i_1, i_2, \dots, i_k)} f_i w_i \oplus \sum_{i \in (i_1, i_2, \dots, i_k)} (1 \oplus f_i) w_i \\ &= \sum_{i \notin (i_1, i_2, \dots, i_k)} f_i w_i \oplus (1 \oplus f_{i_1}) w_{i_1} \oplus (1 \oplus f_{i_2}) w_{i_2} \\ &\quad \oplus \dots \oplus (1 \oplus f_{i_k}) w_{i_k} \\ &= \sum_{i=1}^{2L+1} f_i w_i \oplus (w_{i_1} \oplus w_{i_2} \oplus \dots \oplus w_{i_k}) \\ &= s^T \oplus d \end{aligned}$$

则由式 (4) 可得:

$$Wg^T = s^T \oplus d = s^T \oplus c^T \oplus s^T = c^T$$

用该方法, 可在  $(2L + 1)$  bits 宿主的可修改数据中嵌入  $2L$  bits 数据, 且最多只需修改  $L$  bits 宿主信息。

#### 4.2 $m = 2L, n > (2L + 1)$ 时, 隐秘信息的嵌入/提取

由式 (3) 和式 (4) 可知,  $d^T$  始终为  $2L$  维行矢量, 对任意的  $2L$  维行矢量  $d^T$ , 若为使其满足  $d = w_{i_1} \oplus w_{i_2} \oplus \dots \oplus w_{i_k}$  ( $w_{i_1}, w_{i_2}, \dots, w_{i_k}$  分别为从矩阵  $W$  中选出的  $k$  列), 则式 (2) 中的每一列矢量至少在矩阵  $W_{2L \times n}$  中出现一次, 其余的列矢量可以是式 (2) 矩阵中的任一列矢量。

由以上分析可知, 由于  $W_{2L \times n}$  矩阵可有  $(2L + 1)! \cdot C_n^{(2L+1)} \cdot (2L + 1)^{(n-2L-1)}$  种选择, 因此当  $n$  较大时, 这是一个很大的数, 而且  $W_{2L \times n}$  矩阵可用做密钥。

此情况的不同矩阵  $W_{2L \times n}$  的嵌入/提取方法与 4.1 节论述基本一样, 只需要稍微进行些调整即可。

### 5 实验及结果

为了验证上述方法的效果, 本文在局域网中进行了模拟实验, 实验工作平台为 Window XP 下的 Visual C++ 6.0 软件和 Matlab 软件, 实验结果表明, 效果较好, 以下给出部分实验结果。

### 5.1 视频中隐藏 low level 视频数据

图版 I 图 1 和图 2 给出了在 main level MPEG-II 彩色视频中隐藏 low level MPEG-II 彩色视频的实验结果。数据嵌入过程中以一个  $8 \times 8$  图像块为单元, 嵌入 low level MPEG-II 彩色视频时, 先对其进行部分解压, 再从图像块 DCT 域的中高频部分选择出 33 个系数, 由于在其中最多可修改 16 个系数的最低位, 因此可嵌入 32bits 数据。若 main level MPEG-II 视频为  $720 \times 480 \times 30$  (YUV:4:2:0) 时, 则可嵌入的最大数据流为 7.77Mb/s 左右数据。实验所用视频均为 MPEG-II 官方网站下载的测试视频 (图版 I 图 1 和图 2)。

宿主视频 Mobl\_120 (12Mb/s) 每帧大小为  $704 \times 480$ , 共 450 帧; 待隐藏视频 Flwr\_015 (1.5Mb/s) 每帧大小为  $352 \times 240$ , 共 450 帧。其中图版 I 图 1(a) 为未隐藏数据时, 两帧原始宿主视频图像

帧, 图版 I 图 1(b) 为隐藏有 low level 视频的相应视频图像帧。图版 I 图 1 表明, 隐藏信息前与隐藏信息后的宿主视频图像, 用人眼很难分辨出差异, 有着较好的视觉效果。图版 I 图 2(a) 为其中待隐藏的两帧原始 low level 视频图像帧, 图版 I 图 2(b) 为经隐秘传输后提取出的两帧相应 low level 视频图像帧。图版 I 图 2 表明, 原始 low level 图像帧和经隐秘传输后, 其提取出的相应 low level 图像帧相同。

表 1 给出了在两个不同压缩比的 MPEG-II 视频段 (视频每帧大小为  $704 \times 480$ ) 中嵌入 low level 视频段 (Flwr\_015 (1.5Mb/s) 的一组实验统计结果。实验数据表明, 上述的隐藏方法可以嵌入较大容量的数据, 其不仅数据嵌入率较高, 且有较好的平均峰值信噪比。实验过程中, 当没有考虑噪声及远距离传输对数据的影响效果时, 其正确提取率均为 100%。

表 1 不同视频隐藏 low level 视频实验相关数据

Table 1 Experimental data based on different videos hiding low level video

宿主视频	视频帧数	嵌入数据大小 (Mb)	数据嵌入的平均码率 (Mb/s)	原视频大小 (Mb)	嵌入数据后视频大小 (Mb)	平均峰值信噪比 (dB)
Mobl_080 (8.0Mb/s)	450	20.31	1.35	15.00	16.87	26.80
Mobl_120 (12.0Mb/s)	450	26.13	1.74	22.53	24.38	28.79
Mobl_180 (18.0Mb/s)	450	39.60	2.64	34.27	37.08	30.17
Mobl_400 (40.0Mb/s)	450	44.51	2.97	75.08	75.86	34.66
Tens_080 (8.0Mb/s)	450	22.50	1.50	15.04	17.16	30.05
Tens_120 (12.0Mb/s)	450	27.76	1.85	21.55	24.53	31.44
Tens_180 (18.0Mb/s)	450	40.74	2.71	34.56	37.71	33.02
Tens_400 (40.0Mb/s)	450	45.60	3.04	75.30	76.06	34.69

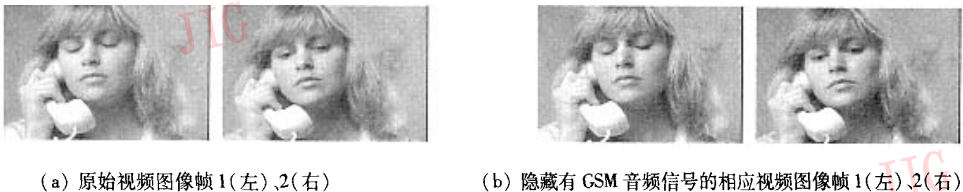
### 5.2 视频中隐藏 GSM 编码语音

图 2 是在 MPEG-II 视频段 Susi\_040 (4.0Mb/s) 中隐藏 GSM (global system for mobile communication) 编码音频信号的实验结果, 其数据嵌入方法和上述 MPEG-II 视频中嵌入 low level 视频的方法相同。其中 Susi\_040 (4.0Mb/s) 视频每帧大小为  $704 \times 480$ , 共 450 帧, 压缩比 120:1; 选用的音频信号为 8s 的 GSM 语音信号, 共 64000 个样点。

图 2(a) 为未隐藏信息时, 其中两帧原始视频图像, 图 2(b) 为隐藏信息后相应的视频帧; 图 2 表明,

隐藏信息前与隐藏信息后的视频图像, 用人眼很难分辨出差异。图 3(a) 为原始 PCM (plus code modulation) 语音信号, 图 3(b) 为待隐藏的 GSM 语音解码后的 PCM 语音信号, 图 3(c) 为提取的 GSM 语音经解码恢复后的 PCM 语音信号, 其中横轴是样点个数, 纵轴是幅值 (单位为  $5V/2^{16}$ )。实验数据表明, 待隐藏的原始 GSM 语音数据和嵌入提取后所得的 GSM 语音数据完全相同。

表 2 给出了在两个不同压缩比的 MPEG-II 视频段 (Flwr\_015 和 Susi\_015 视频每帧大小为



(a) 原始视频图像帧 1(左)、2(右)

(b) 隐藏有 GSM 音频信号的相应视频图像帧 1(左)、2(右)

图 2 原始视频帧和隐藏数据后的相应视频图像帧

Fig. 2 Frames of original video and relevant frames of video hiding data

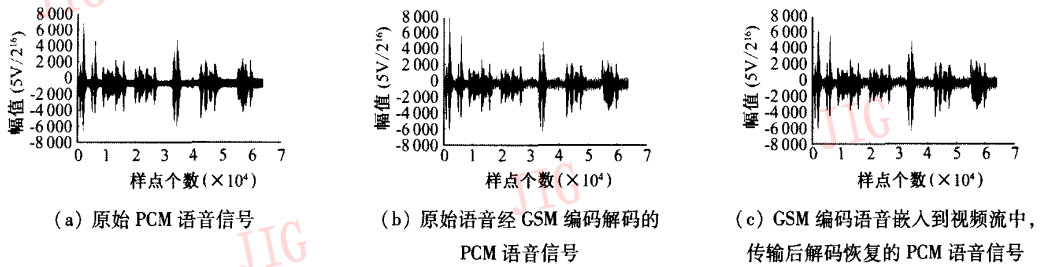


图 3 语音信号波形对比图

Fig.3 Contrastive wave of speech signal

表 2 不同视频隐藏 GSM 语音信号的实验数据

Table 2 Experimental data based on different videos hiding GSM wave signal

宿主视频	视频帧数	嵌入数据大小 (Mb)	数据嵌入的平均码率 (Mb/s)	原视频大小 (Mb)	嵌入数据后视频大小 (Mb)	平均峰值信噪比 (dB)
Flwr_015 (1.5Mb/s)	450	4.08	0.27	2.82	3.22	23.44
Flwr_040 (4.0Mb/s)	450	13.28	0.89	7.53	9.47	24.03
Flwr_060 (6.0Mb/s)	450	18.08	1.21	11.29	13.54	26.60
Flwr_080 (8.0Mb/s)	450	21.87	1.46	15.05	17.37	27.40
Susi_015 (1.5Mb/s)	450	5.28	0.35	2.82	3.49	28.41
Susi_040 (4.0Mb/s)	450	17.10	1.14	7.52	10.32	34.30
Susi_060 (6.0Mb/s)	450	22.4	1.49	11.29	14.36	34.75
Susi_080 (8.0Mb/s)	450	26.04	1.74	15.04	18.01	35.44

352 × 240,其余视频每帧大小为 704 × 480)中嵌入 GSM 编码语音的一组实验数据。从表中数据可知,视频流中具有较高的平均数据嵌入率和较好的平均峰值信噪比,在没有考虑噪声及远距离传输的影响时,具有 100%的正确提取率。

## 6 结论

本文给出了一个将 low level MPEG-II 彩色视频隐藏在另一路 main level MPEG-II 视频中的隐秘传输方案及一种新的数据隐藏方法,用该方法可在  $(2L + 1)$  bits 宿主可修改矢量中,嵌入  $2L$  bits 数据,而且最多只需修改  $L$  bits 宿主信息。由于它具有较高数据嵌入率,因此适用于流媒体及信息量较大信息的隐藏及隐秘传输,且在嵌入过程中可对待隐藏信息数据进行加密和可利用  $W_{m \times n}$  矩阵的多选择性作为另外一个密钥,这就使得隐藏的数据在传输过程中具有较好的安全性。

该方法在计算机上进行了模拟实验,对 low level MPEG-II 彩色视频数据和 GSM 编码音频信号隐藏在 main level MPEG-II 彩色视频数据的实验结果表明,该方法较好地解决了视频待藏数据量较大及隐蔽性的矛盾,且其嵌入/提取步骤简单有效,易

于实现。

本文主要讨论将 low level MPEG-II 彩色视频数据及较大信息量信息隐藏在 main level MPEG-II 彩色视频数据中的嵌入/提取方法,但噪声及信息在传输中的其他因素对该方法的影响尚需进一步研究。

## 参考文献 (Reference)

- 1 Frank Hartung, Bernd Girod. Watermarking of uncompressed and compressed video[J]. Signal Processing, 1998, 66(3):283 ~ 301.
- 2 Lu Hong-lin, Cheng Yi-ming, Wang Yi-xiao, et al. A secret transmission method based on ICA for Chinese characters[J]. Journal of Chinese Information Processing, 2003, 17(4):59 ~ 65. [陆红琳,程义民,王以孝等.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 Transactions on Communications, 2002, 50(8):1227 ~ 1231.
- 4 Galand F, Kabatiensky G. Information hiding by coverings [A]. In: Proceedings of Information Theory Workshop [C], Paris, 2003: 151 ~ 154.
- 5 Wu Chung-ping, Kuo C-C J. Fragile speech watermarking for content integrity verification [A]. In: IEEE International Symposium on Circuits and Systems [C], Phoenix-Scottsdale, AZ, USA, 2002, 2: 436 ~ 439.



图1 用于边缘检测的3幅彩色原始图像

Fig.1 Original image used in color edge detection

程义民等：一种彩色视频信息的隐秘传输方法



图1 原始视频帧和隐藏数据后视频帧的比较

Fig.1 Contrast between frames of original video and relevant frames of video hiding data

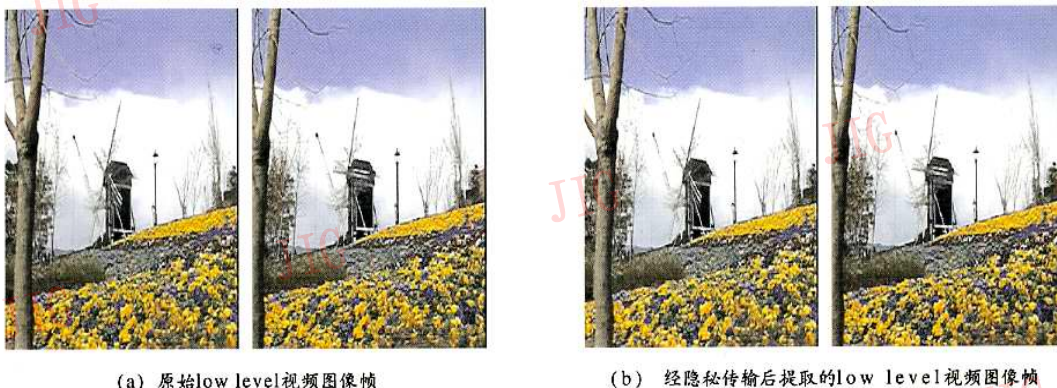


图2 原始low level视频帧和经隐秘传输后提取的low level视频帧的比较

Fig.2 Contrast between frames of original video and relevant extracted frames of low level video through covert communication