

文章编号:1001-9081(2010)11-3022-03

## 基于运动矢量的视频隐写方法

相丽<sup>1</sup>, 潘峰<sup>1,2</sup>, 钮可<sup>1</sup>, 郭耀<sup>1</sup>

(1. 武警工程学院 网络与信息安全武警部队重点实验室, 西安 710086;

2. 武警工程学院 信息安全研究所, 西安 710086)

(xiangli905@sohu.com)

**摘要:**为减小秘密信息嵌入对载体视频的修改率,提出了一种基于运动矢量及线性分组码的视频隐写方法。该方法在原始视频进行H.264压缩过程中将秘密信息嵌入到其运动矢量中。线性分组码的使用不仅可大幅提高载体视频的运动矢量利用率,而且可有效降低运动矢量修改率。所提算法不仅具有计算复杂度低、视觉不可见性高的特点,而且可以实现秘密信息的盲提取。实验表明,该方法在保持良好的视频质量的前提下,可以满足隐蔽通信对于高嵌入容量的需求。

**关键词:**视频隐写;运动矢量;线性分组码

**中图分类号:**TP391.41 **文献标志码:**A

## Video steganography based on motion vector

XIANG Li<sup>1</sup>, PAN Feng<sup>1,2</sup>, NIU Ke<sup>1</sup>, GUO Yao<sup>1</sup>

(1. Key Laboratory of Network and Information Security Under the Chinese Armed Police Force,  
Engineering College of the Armed Police Force, Xi'an Shaanxi 710086, China;

2. Institute of Information Security, Engineering College of Chinese Armed Police Force, Xi'an Shaanxi 710086, China)

**Abstract:** In order to reduce the modification rate of cover media which is caused by embedding process, a new video steganography scheme based on motion vectors and linear block codes was proposed in this paper. The method embedded secret messages in the motion vectors of cover media during the process of H.264 compressing. Linear block codes were used to increase the utilization rate and reduce the modification rate of the motion vectors. The proposed steganographic scheme not only has lower computational complexity, but also is highly imperceptible to human being. Furthermore, the secret information can be extracted directly without using the original video sequences. Experiments were designed to prove the feasibility of the proposed method. The experimental results show that the proposed scheme can embed large amounts of information and can maintain good video quality as well.

**Key words:** video steganography; motion vector; linear block code

## 0 引言

近年来,随着网络通信技术及信息处理技术的发展,视频隐写技术作为一种新的信息安全技术得到了较快的发展。视频隐写技术通常是与视频压缩过程紧密联系在一起的。视频压缩大多是通过计算运动矢量来消除帧间冗余信息。运动矢量是视频编码流或压缩码流中的重要信息,可将其作为视频隐写的嵌入点。

基于运动矢量的视频隐写算法通常综合利用运动矢量的幅值、相位、方向、水平分量和垂直分量等元素来嵌入秘密信息。许多针对MPEG压缩的基于运动矢量的信息隐藏方法已被提出<sup>[1-2]</sup>。Jordan等人<sup>[3]</sup>利用MPEG视频序列的帧间信息将秘密信息隐藏在数字视频中,但此法的秘密信息嵌入容量不高,使其在隐蔽通信过程中的应用受到一定限制。Ding等人<sup>[4]</sup>提出了一种基于运动矢量相位差的信息隐藏算法,可在两个运动矢量中嵌入1比特数据,但该方法存在载体利用率不高且运动矢量修改过多的问题。

为解决文献[4]中载体利用率不高及运动矢量修改率过

多的问题,本文提出了基于运动矢量及线性分组码的视频隐写算法。将线性分组码应用于视频隐写过程中,不仅可有效降低运动矢量的修改率,而且可提高载体视频的利用率。实验表明,该算法不仅具有计算复杂度低、视觉不可见性好的特点,而且能够满足隐蔽通信对于高嵌入容量的需求。

## 1 基于运动矢量的视频隐写算法

### 1.1 线性分组码<sup>[5]</sup>

线性码是指监督码元与信息码元之间的关系是线性关系,即它们的关系可用一组线性代数方程联系起来。分组码是将 $k$ 个信息码元划分为一组,然后由这 $k$ 个码元按照一定的规则产生 $r$ 个监督码元,从而组成长度为 $n = k + r$ 的码组。在分组码中,监督码元仅监督本码组中的信息码元。分组码一般用符号 $(n, k)$ 表示,并且将分组码的结构规定为前面 $k$ 位是信息位,后面附加 $r(r = n - k)$ 个监督位。若 $r$ 个附加码元是由信息码元的线性运算产生的,则此码叫做 $(n, k)$ 线性分组码。在信道编码中,定义码字中非零码元的数目为码字的汉明重量,简称码重。把两个码字之间对应码位上具有不同二元码元的位

收稿日期:2010-05-30;修回日期:2010-07-10。

基金项目:国家自然科学基金资助项目(60842006);武警工程学院基础研究基金资助项目。

作者简介:相丽(1987-),女,山东临沂人,硕士研究生,主要研究方向:信息隐藏;潘峰(1967-),男,陕西西安人,副教授,主要研究方向:信息安全、多媒体处理;钮可(1981-),男,浙江湖州人,助教,主要研究方向:视频隐写、数字水印;郭耀(1984-),男,陕西三原人,助教,主要研究方向:数字水印。

数定义为两码字的汉明距离,简称码距。在线性分组码 $(n, k)$ 中,监督码元和信息码元间是线性关系,可表示为 $HC^T = 0^T$ ,其中 $H$ 称为 $(n, k)$ 线性码的一致监督矩阵, $C$ 为某码组。

设 $C$ 是 $GF(2)$ 上的一个 $(n, k)$ 码, $j$ 是长为 $n$ 的任意向量,则将集合 $j + C = \{j + x \mid x \in C\}$ 称为 $C$ 的一个陪集。陪集具有如下性质:

- 1) 任意长为 $n$ 的向量都属于 $C$ 的某个陪集;
- 2) 每个陪集恰好包含 $2^k$ 个向量;
- 3) 两个陪集或者不相交或者完全重合(不可能部分相交)。

一个陪集中具有最小重量的向量称为陪集首。如果多于一个向量具有最小重量,则从中随机选择一个定为陪集首。

一个 $(n, k)$ 码组 $C$ 的标准阵列是一个 $GF(2^n)$ 上全部向量的 $2^{n-k} \times 2^k$ 阵列,它的第一行由码组 $C$ 构成(0码字在最左边),其他行是陪集 $j_i + C$ ,都以相应次序排列,陪集首放在最左边。标准阵列的每一行为码的一个陪集,每个陪集有相同的错误图样。由于陪集首是可纠的错误图样,为了使译码错误概率最小,所以在构造标准阵列时是选取重量最轻的 $n$ 重码字作陪集首。这样,当错误图样为陪集首(可纠的错误图样)时,接收码字与发送码字间的距离(等于陪集首)最小。

$s$ 为码字的伴随式,伴随式仅与错误图样有关,不同的错误图样具有不同的伴随式。在标准阵列中,一个陪集的所有 $2^k$ 个 $n$ 重码字具有相同的伴随式,不同陪集的伴随式互不相同。陪集中任意变量的伴随式等于陪集首的伴随式,因此,同一陪集中所有变量伴随式相同。而不同陪集中,由于陪集首不同所以伴随式不同。任意 $n$ 重码字的伴随式决定于它在标准阵列中所在陪集的陪集首;标准阵列的陪集首和伴随式是一一对应的,因而码的可纠错误图样和伴随式也是一一对应的。

## 1.2 秘密信息嵌入算法

本文选择在原始视频的 H. 264 压缩过程中实现秘密信息的嵌入。具体嵌入过程如下(第1)~(4)步同文献[4]):

- 1) 指定宏块范围,不考虑位于视频边界的宏块。
- 2) 计算符合上面条件宏块的运动矢量幅度。
- 3) 根据已经选定的阈值 $L$ 筛选出幅度大于此阈值的运动矢量:

$$G = \{MV_0, MV_1, \dots, MV_{N-1}\}; |G| = N$$

其中: $(MV_{iv}^2 + MV_{ih}^2) \geq L (0 \leq i \leq N)$ ,  $MV_{ih}$ 与 $MV_{iv}$ 分别是运动矢量 $MV_i$ 的水平分量和垂直分量。

- 4) 计算 $G$ 中每个运动矢量的相位:

$$\varphi_i = \arctan(MV_{iv}/MV_{ih}); 0^\circ \leq \varphi_i \leq 360^\circ$$

5) 将 $(0^\circ, 360^\circ]$ 划分为8个不重复不遗漏的区间,如图1所示。若某一个运动矢量的相位属于图中空白区域,则其代表数据1;反之,若属于阴影部分则代表数据0。

6) 将 $N$ 个运动矢量组成的二进制比特流按每组 $n$ 比特进行分组,记为 $q$ 。

7) 将待嵌入的秘密信息按每组 $(n-k)$ 比特进行分组,记为 $a$ 。

- 8) 计算 $q$ 的伴随式, $s = qH^T$ 。

9) 计算 $b = s \oplus a$ ,查询陪集首与伴随式的对应表,寻找和 $b$ 对应的陪集首,假设为 $e_b$ 。

10) 计算 $q' = q \oplus e_b$ , $q'$ 即为嵌入秘密信息后的运动矢量组成的二进制比特流。

在隐写过程中将线性分组码的监督矩阵 $H$ 以及运动矢

量相位的划分方法作为密钥。

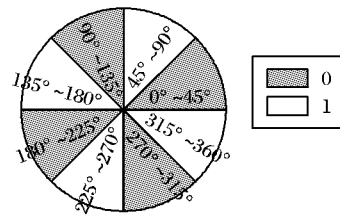


图1 运动矢量相位划分示意图

## 1.3 秘密信息提取算法

秘密信息的提取算法步骤如下:

第1)~6)同秘密信息嵌入算法中的第1)~6),得到 $q'$ 。

7) 计算 $s' = q' H^T = qH^T \oplus e_b H^T = s \oplus b = s \oplus s \oplus a = a$ , $s'$ 即为嵌入的秘密信息,从而实现了秘密信息的盲提取。

## 2 举例

本文选择将 $(6, 2)$ 线性分组码应用于秘密信息的嵌入过程中,其监督矩阵 $H$ 如下所示。

$$H = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

陪集首与伴随式的对应关系如表1所示。假设经过计算后运动矢量根据其相位组成二进制序列 $q = 011000100101$ ,将其分组为 $q_1 = 011000$ , $q_2 = 100101$ 。秘密信息为 $a = 01110101$ ,将其分组为 $a_1 = 0111$ , $a_2 = 0101$ 。

表1  $(6, 2)$ 码陪集首与伴随式对应关系

陪集首( $e_i$ )	伴随式( $s_i$ )	陪集首( $e_i$ )	伴随式( $s_i$ )
000000	0000	001000	1000
000001	0001	001001	1001
000010	0010	100000	1010
000011	0011	100001	1011
000100	0100	001100	1100
010000	0101	011000	1101
000110	0110	100100	1110
010010	0111	110000	1111

按如下步骤实现秘密信息的嵌入:

- 1) 计算 $s_1 = q_1 H^T = 1101$ 。
- 2)  $b_1 = s_1 \oplus a_1 = 1010$ ,查表1得 $e_b = 100000$ 。
- 3) 计算 $q'_1 = q_1 \oplus e_b = 111000$ ,同样,可以计算出 $q'_2 = 000101$ ,因此嵌入秘密信息后的比特流为 $q' = 111000000101$ 。

从以上过程容易看出,嵌入8比特秘密信息后的 $q'$ 与原始比特流 $q$ 只有2比特不同,因此载体修改率较低。

秘密信息的提取只需在获得 $q'$ 后计算 $a'_1 = q'_1 H^T = 0111$ , $a'_2 = q'_2 H^T = 0101$ 即可,这样秘密信息 $a = 01110101$ 即被提取出来。

从秘密信息嵌入算法中的第10)步可知, $q' \oplus q = e_b$ ,即信息隐藏对视频运动矢量带来的变化为 $e_b$ ,而 $e_b$ 属于陪集首集合, $e_b$ 的重量等于嵌入过程中修改的运动矢量数目,故嵌入 $(n-k)$ 比特信息对 $n$ 个运动矢量的修改个数取决于陪集首的分布,最大修改数目为最重的陪集首的重量,最小修改数目为0。

### 3 实验

本文实验所用电脑配置为 Core2 6320 CPU (1.8 GHz), 1.0 GB RAM, 使用 VC++ 6.0 进行仿真实验。实验中选取标准的 YUV 格式视频序列 Flower (250 帧,  $352 \times 288$ ) 和 Foreman (300 帧,  $176 \times 144$ )。实验中分别采用本文方法与文献[4]方法在原始视频 H. 264 压缩过程中嵌入秘密信息, 并将实验结果进行了对比。

#### 3.1 嵌入容量

实验中设定  $L=10$ , 按照如图 1 所示方法将  $(0^\circ, 360^\circ]$  划分成 5 个不重复不遗漏的区间, 采用 (6, 2) 线性分组码即可在 6 个运动矢量中嵌入 4 比特的秘密信息, 嵌入容量最大可达到视频中运动矢量总数的  $2/3$ 。而文献[4]中嵌入 1 比特秘密信息需利用 2 个运动矢量, 故本文算法较文献[4]而言, 不仅在运动矢量的利用率方面而且在整体的嵌入容量上均有所改进。

#### 3.2 载体修改率

由于本文算法是基于线性分组码且对载体的修改率是由陪集首的最大重量决定的, 因此本文算法具有修改率低的特点。文献[6]中定义运动矢量修改率如下所示:

运动矢量修改率 = 修改的运动矢量数目 / 嵌入的比特数

按照上式的计算方法, 文献[4]的最大运动矢量修改率为 1 而本文算法的最大运动矢量修改率为  $1/2$ , 最小修改率为 0。因此本文算法的修改率明显低于文献[4]中提出的算法。

#### 3.3 视觉不可见性

选择在压缩过程中进行秘密信息的嵌入以及线性分组码的使用使得本文算法可取得较好的视觉不可见性效果。表 2 为分别利用文献[4]及本文算法嵌入秘密信息后 Flower 和 Foreman 视频序列中对应图像帧的峰值信噪比 PSNR 平均值。PSNR 常用来衡量嵌入秘密信息后图像的质量, PSNR 越高, 表明信息嵌入后对原待嵌入信息的图像带来的噪声越小, 也就是隐藏的效果越好。

表 2 视频序列的 PSNR 平均值

视频序列		PSNR/dB	
		文献[4]方法	本文方法
Flower	1 ~ 50 帧	37.631	38.132
	51 ~ 100 帧	37.182	37.425
	101 ~ 150 帧	36.532	37.254
	151 ~ 200 帧	36.653	37.195
	201 ~ 250 帧	36.438	37.261
Foreman	1 ~ 50 帧	40.954	42.008
	51 ~ 100 帧	39.101	41.415
	101 ~ 150 帧	38.194	41.392
	151 ~ 200 帧	37.238	40.623
	201 ~ 250 帧	36.856	40.224
	251 ~ 300 帧	36.465	39.385

一般, 当 PSNR 值大于 30 dB 时, 人眼就难以分辨出两幅图像处理前后的差异<sup>[7]</sup>。从表 2 可以看出, 表中的 PSNR 平均值都在 30 dB 以上, 且本文方法的 PSNR 平均值均大于文献[4]方法, 说明本文算法对秘密信息的隐藏效果较好, 在嵌入秘密信息后, 不会造成视频质量的明显下降, 较文献[4]而言, 可以获得更为满意的视觉不可见性效果。

图 2~3 分别为在 Flower、Foreman 视频序列中采用文献

[4]及本文算法嵌入秘密信息后所得 PSNR 值的比较。

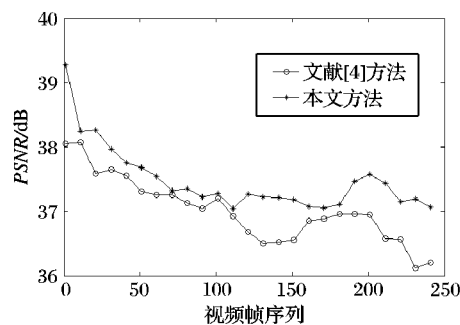


图 2 Flower 视频序列的 PSNR 值对比

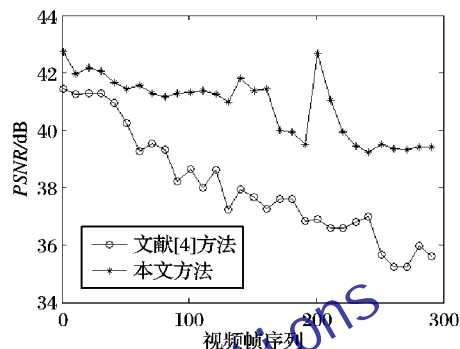


图 3 Foreman 视频序列的 PSNR 值对比

### 4 结语

本文算法选择在原始视频进行 H. 264 压缩过程中将秘密信息嵌入到其运动矢量中。利用线性分组码进行秘密信息的嵌入不仅可有效降低载体视频的运动矢量修改率而且提高了载体利用率。该算法不仅具有计算复杂度低、不可见性高的特点, 而且可以实现秘密信息的盲提取。实验表明, 该方法可以满足隐蔽通信对于高嵌入容量的需求, 并且可以保持良好的视频质量。

#### 参考文献:

- [1] ZHANG JUN, LI JIEGU, ZHANG LING. Video watermark technique in motion vector [C]// Proceedings of XIV Symposium on Computer Graphics and Image Processing. Washington, DC: IEEE, 2001: 179-182.
- [2] BODO Y, LAURENT N, DUGELAY J L. Watermarking video: Hierarchical embedding in motion vectors [C]// IEEE Proceedings of International Conference on Image Processing. Washington, DC: IEEE, 2003: 739-742.
- [3] JORDAN F, KUTTER M, EBRAHIMI T. Proposal of a watermarking technique for hiding/retriving data in compressed and decompressed video [EB/OL]. [2009-12-12]. <http://www.alpvision.com/pdf/mvt.pdf>.
- [4] DING Y F, LONG W C. Data hiding for digital video with phase of motion vector [C]// Proceedings of 2006 IEEE International Symposium on Circuits and Systems. Washington, DC: IEEE, 2006: 1422-1425.
- [5] 田丽华. 编码理论[M]. 2 版. 西安: 西安电子科技大学出版社, 2007: 116-134.
- [6] HE XUENSEN, LUO ZHUN. A novel steganographic algorithm based on the motion vector phase [C]// 2008 International Conference on Computer Science and Software Engineering. Washington, DC: IEEE, 2008: 822-825.
- [7] 宣曼. H. 264 标准中数字视频水印技术的研究[D]. 合肥: 合肥工业大学, 2007.