

基于运动矢量相位角和卷积码的大容量视频隐写算法

杨 鹏¹, 魏立线^{1,2}, 杨晓元^{1,3}

(1. 武警工程学院 电子技术系, 西安 710086; 2. 武警工程学院 网络与信息安全研究所, 西安 710086;

3. 西安电子科技大学 网络信息安全教育部重点实验室, 西安 710071)

(wjbird2008@126.com)

摘 要:为提高视频隐写中秘密信息的嵌入容量,提出一种基于运动矢量相位角和卷积码的大容量视频隐写算法。通过研究视频流中每一个帧组里的P帧和B帧上的运动信息,将秘密信息经过交织变换,用相位角的值表示不同的数字序列并作为卷积码的基本生成矩阵,使用卷积码来嵌入秘密信息。实验表明,该算法具有嵌入容量大、不可见性好和稳健性强等特点,在保持良好视频质量的前提下,可以达到视频隐写中大容量嵌入的目的。

关键词:运动矢量相位角;交织变换;卷积码;大容量;视频隐写

中图分类号: TP309.7 **文献标志码:** A

Big-capacity video steganography based on motion vector phase and convolutional code

YANG Peng¹, WEI Li-xian^{1,2}, YANG Xiao-yuan^{1,3}

(1. Department of Electronic Technology, Engineering College of Armed Police Force, Xi'an Shaanxi 710086, China;

2. Institute of Network and Information Security, Engineering College of Armed Police Force, Xi'an Shaanxi 710086, China;

3. Key Laboratory of Network and Information Security of the Ministry of Education, Xidian University, Xi'an Shaanxi 710071, China)

Abstract: In order to increase the capacity of secret information in video steganography, a big-capacity video steganography algorithm was proposed based on motion vector phase and convolutional code. By studying the moving information of P frame and B frame in every Group of Pictures (GOP), the interlace switch was used to trade with the secret information at first, and then the different size of motion vector phase was used to represent different information to denote the basic generator matrix and the convolutional code was used to insert secret information. The experimental results show that the proposed algorithm not only has a big capacity of insert information, but also has a good imperceptibility and great robustness for secret information. It can achieve high capacity in video steganography and maintain good video quality as well.

Key words: motion vector phase; interlace switch; convolutional code; big capacity; video steganography

0 引言

近年来,随着多媒体技术和网络通信技术的发展,数字图像、音频、视频等各种多媒体不断走进我们的生活,为我们提供更加便捷的服务。基于图像的隐写技术已经发展得比较成熟,但是由于图像载体容量有限,能够嵌入的秘密信息也是有限的。而随着数字技术的不断发展,需要保护秘密信息的容量越来越大。对于某些大容量的信息,数字图像已不能完成对其进行隐密保护,需要有更大容量的载体来承载更多的秘密信息。数字视频相比数字图像具有更大的载体容量,在视频通信中嵌入秘密信息也是保密通信的重要手段。视频隐写技术具有嵌入容量大、通信质量高、稳健性强等特点,已被越来越多的人重视和研究。运动矢量^[1-2]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可以利用矢量的幅值、相位角、水平分量和垂直分量等来实现秘密信息的嵌入。Xu Changyong等人^[3]提出了在视频压缩后的隐写方法,该方法实现了通过修改运动矢量大小来实现在P帧和B帧上嵌入秘密信息,但该算法稳健性欠佳。Ding Yu-Fang等人^[4]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1b数据,其不足之处是载体利用率不高。

卷积码^[5-6]具有较强的纠错能力,而交织技术^[5-6]能有效抵抗持续时间的突发性误码。文献[7]中使用交织技术和卷积码仅对原始水印信息进行处理,没有与载体信息进行作用。本文将卷积码和交织技术运用于视频隐写过程中,提高了视频隐写的稳健性,并在一个扇区代表多位嵌入信息,有效提高了载体的利用率,有大容量的特点。实验证明,该算法不仅具有视频不可见性好、秘密信息稳健性强的特点,而且还可以满足保密通信对大容量嵌入的需求,有效提高载体利用率。

1 卷积码和交织技术

1.1 卷积码

卷积码主要用于前向纠错的通信系统中,而且卷积码不同于分组码之处在于:在任意给定时间单元时刻,编码器输出的 n_0 个码元中,每一个码元不仅和此时此刻输入的 k_0 个信息有关,还与前连续 m_0 个时刻输入的信息元有关。

设卷积码编码器输入码序列(待编码的信息序列)为:

$$U = [u_0(1) u_0(2) \cdots u_0(k_0) u_1(1) u_1(2) \cdots]$$

收稿日期:2010-10-20;修回日期:2010-12-08。

基金项目:国家自然科学基金资助项目(60842006);武警工程学院基础基金项目(wjy201027)。

作者简介:杨鹏(1985-),男,湖北仙桃人,硕士研究生,主要研究方向:信息隐藏; 魏立线(1966-),男,陕西户县人,教授,主要研究方向:信息安全; 杨晓元(1959-),男,湖南湘潭人,教授,主要研究方向:信息安全、密码学。

$$u_1(k_0) \cdots u_s(1) u_s(2) \cdots u_s(k_0) \cdots]$$

编码器输出码序列为:

$$C = [c_0(1) c_0(2) \cdots c_0(n_0) c_1(1) c_1(2) \cdots c_1(n_0) \cdots c_s(1) c_s(2) \cdots c_s(n_0) \cdots]$$

编码器输出码序列中任一子码可以由如下卷积关系给出(矩阵表示):

$$C = UG_{\infty} \quad (1)$$

其中: U 为输入序列, G_{∞} 为生成矩阵, C 为输出序列。

1.2 交织技术

交织是一种能有效抵抗持续时间的突发性误码的编码技术。其基本原理是:在发送端将原本顺序的比特流按照一定规律打乱后输出,在接收端再按照相同的规律将接收到的数据恢复成原来的顺序。交织技术的种类有很多,本文采用行列交换交织技术,即对于卷积编码后的秘密信息比特流,将其排列成矩阵形式,然后进行行列交换输出码流。

例如:输入序列 M , 长为 $m \times n$, 将此序列按照 m 行, n 列矩阵排列。得矩阵如下:

$$\begin{bmatrix} M_1 & M_2 & \cdots & M_n \\ M_{n+1} & M_{n+2} & \cdots & M_{2n} \\ \vdots & \vdots & & \vdots \\ M_m & M_{m+1} & \cdots & M_{m \times n} \end{bmatrix}$$

当读取时采取最简单的行列交织读取,即读取顺序为:

$M_1, M_{n+1}, \cdots, M_m; M_2, M_{n+2}, \cdots, M_{m+1}; \cdots; M_n, M_{2n}, \cdots, M_{m \times n}$ 。记此序列经交织变换后的序列为 M' 。

2 基于运动矢量相位角的视频隐写算法

2.1 秘密信息的嵌入算法

H. 264 视频压缩标准在对视频压缩时对每帧视频图像进行分块处理,以块为单位进行压缩。选择合适的运动宏块,对秘密信息的保护至关重要。本文根据运动矢量模长的大小来判断运动矢量的信息,给定一个阈值,通过与阈值大小相比来确定该运动矢量是否适合嵌入秘密信息。具体选择步骤如下:

1) 从视频流中分离出 P 帧和 B 帧图像,通过 H. 264 压缩编码标准来确定出该帧的运动宏块,并得到每个宏块的运动矢量 $P_{MV}[i]$ ($0 < i < N_{MB}, N_{MB}$ 是此帧的运动矢量的总数)。

2) 计算出该矢量的模长 $|P_{MV}[i]| = \sqrt{H^2[i] + V^2[i]}$, $H[i]$ 表示运动矢量 $P_{MV}[i]$ 的水平分量, $V[i]$ 表示运动矢量 $P_{MV}[i]$ 的垂直分量。

3) 给定一个运动矢量阈值 ε , 记 $MB[i]$ 表示为第 i 块运动宏块是否适合嵌入秘密信息,判定如下: $MB[i] = \begin{cases} 1, & |P_{MV}[i]| > \varepsilon \\ 0, & |P_{MV}[i]| \leq \varepsilon \end{cases}$, $MB[i] = 1$ 表示此宏块适合嵌入秘密信息,记为有效宏块; $MB[i] = 0$ 表示此宏块不适合嵌入秘密信息,记为无效宏块。

4) 对每一帧中所有的运动宏块重复上述计算,直到一个帧组中的所有有效宏块全部找出为止。假设整个视频流中找到有效宏块个数为 N 。

在秘密信息的嵌入时,本文采取的策略为将运动矢量相位平均划分为 8 个等大小的角度,根据每个相位角所处范围表示不同的数字序列(如表 1)。

5) 计算出有效宏块的相位角: $\theta(i) = \arctan\left(\frac{V(i)}{H(i)}\right)$, 由

$\theta(i)$ 来确定嵌入信息, $\theta(i)$ 角度范围与数字序列对应关系如表 1 所示。

表 1 三位八个扇区的信息分布

扇区数	相位角范围/(°)	表示信息值
1	0 ~ 45	000
2	45 ~ 90	001
3	90 ~ 135	010
4	135 ~ 180	011
5	180 ~ 225	100
6	225 ~ 270	101
7	270 ~ 315	110
8	315 ~ 360	111

6) 由于一共找到 N 个有效宏块,故形成的 0、1 序列长为 $3N$, 记此序列为 g , 以此作为卷积码编码的基本生成矩阵 g_{∞} , 从而可以得到生成矩阵 G_{∞} 。

7) 假设初始秘密信息序列为 M , 按照一步交织转换得到新的序列为 M' 。

8) 将序列 M' 作为输入序列, 由序列基本生成矩阵 g_{∞} 产生的矩阵 G_{∞} 为生成矩阵, 利用式(1)计算: $g' = M'G_{\infty}$, 则 g' 为带有秘密信息的运动矢量的二进制比特流。

9) 缩短被修改比特组对应宏块运动矢量幅值,使其成为无效宏块。同时在新的对应扇区寻找一个无效宏块,增加其运动矢量幅值,使其成为有效宏块,达到秘密信息在载体信息上的嵌入。

在隐写过程中将基本生成矩阵 g_{∞} , 交织变换中 $m \times n$ 矩阵的行数 m 、列数 n 作为密钥。

2.2 秘密信息的提取

1) 宏块的选择与嵌入算法的步骤 1) ~ 4) 相同;

2) 与嵌入算法步骤 5)、6) 相同,从带有秘密信息的视频载体中,提取带有秘密信息的运动矢量二进制比特流 g' ;

3) 利用密钥 g_{∞} 采用维特比译码算法得到经交织变换后的序列 M' ;

4) 根据交织变换矩阵行列数(m 和 n),经逆向交织变换得到序列 M 。

3 举例说明

本文选择使用(3,1,2)卷积码进行秘密信息的嵌入,假设原始输入信息序列 $M = [101 \ 101 \ 010]$, 行列交织矩阵选择为 3×3 , 即 $m = 3, n = 3$, 假设从载体视频所得运动块所得载体序列 $g = [111 \ 010 \ 001]$ 。

按如下步骤进行秘密信息的嵌入。

1) 将原始秘密信息按照 3×3 矩阵先从左到右,再从上至

下进行排列得矩阵 $\begin{bmatrix} 101 \\ 101 \\ 010 \end{bmatrix}$, 经行列交织变换读取,即先从上

至下,再从左至右读取,得 $M' = [110 \ 001 \ 110]$;

2) 计算基本生成矩阵 $g_{\infty} = [111 \ 010 \ 001]$, 从而可

得到生成矩阵 $G_{\infty} = \begin{bmatrix} 111 & 010 & 001 & 000 & 000 \\ 000 & 111 & 010 & 001 & 000 \\ 000 & 000 & 111 & 010 & 001 \end{bmatrix}$ 。

3) 求 $g' = M'G_{\infty}$, 即 $g' = [101 \ 101 \ 010] \cdot$

$$\begin{bmatrix} 111 & 010 & 001 & 000 & 000 \\ 000 & 111 & 010 & 001 & 000 \\ 000 & 000 & 111 & 010 & 001 \end{bmatrix} = [111 \ 010 \ 110], g'$$
 即嵌入
 秘密信息后的载体信息。

4) 相对原始载体信息 g 第三组信息由 001 更改为 110, 落入扇区 7。缩短 001 对应宏块运动矢量幅值, 使其成为无效宏块。同时在扇区 7 内找到一无效宏块, 增加其运动矢量幅值, 使其成为有效宏块。

由以上过程可以看出, 在嵌入 9 b 后的 g' 与原始载体信息相比较仅有 3 b 不同, 因此, 对不可见性效果较好。

对秘密信息的提取时按以下步骤进行。

1) 在得到 g' 后, 利用已知密钥 g_{∞} , 根据维特比译码算法可得到 $M' = [110 \ 001 \ 110]$ 。

2) 根据所知交织矩阵的行列数 m 及 n , 进行行列逆变换, 得到秘密信息 $M = [101 \ 101 \ 010]$, 即恢复出秘密信息 M 。

表2 本文算法中的载体利用率和嵌入量

视频图像序列	载体尺寸	载体大小/KB	阈值	嵌入信息量/KB	载体利用率/%	平均 PSNR/dB
Mother-daughter	352 × 288	44 550	10	10 469	23.5	38.425
Tennis	352 × 288	14 850	10	3 207	21.6	37.568
Foreman	176 × 144	14 850	5	2 331	15.7	41.649
News	176 × 144	11 138	5	1 603	14.4	42.581

选择一组相同视频载体下对秘密信息的嵌入容量与文献[8]进行嵌入容量的比较。比较结果图1所示。

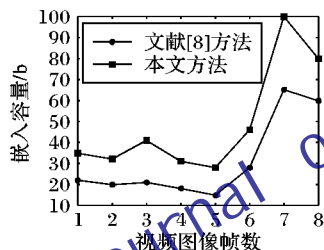
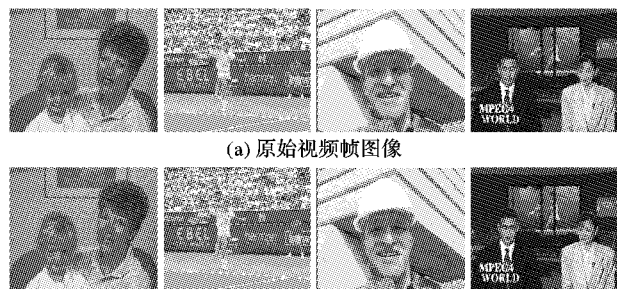


图1 嵌入容量与文献[8]对比

实验结果表明, 在载体利用率和嵌入容量方面, 本文提出的方案都具有较大优势, 更适合于在视频载体上嵌入秘密信息, 对载体具有较高的利用率, 能够实现大容量的目标。

4.2 秘密信息的不可见性

从四组嵌入秘密信息后的视频图像中抽取一帧图像与原始同帧视频图像进行对比, 直观上看, 本文方案具有较好的不可见性, 能够达到在视频图像中嵌入秘密信息的目的。嵌入信息前后的图像如图2所示。



(a) 原始视频帧图像
 (b) 嵌入秘密信息后的视频帧图像
 图2 嵌入秘密信息前后图像对比

4.3 算法的稳健性

实验中, 通过抗二次编码攻击和高斯噪声污染能力检测

从秘密信息的嵌入过程中可以看出, 在嵌入 9 b 秘密信息后, 实际上只使用了 3 个运动矢量信息, 修改了 2 个运动矢量幅值, 达到大容量嵌入的目的。

4 实验仿真

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。实验中选择标准的 YUV 格式视频序列 Mother_daughter(300 帧, 352 × 288), Tennis(300 帧, 352 × 288), Foreman(300 帧, 176 × 144), News(300 帧, 176 × 144) 四组实验视频。实验结果在嵌入容量上与文献[8]进行了对比, 在秘密信息的不可见性上通过与原始信息对比, 稳健性通过二次编码和加入高斯噪声来进行检验。

4.1 嵌入容量

在所选择的四组不同视频载体上, 选择不同的阈值进行仿真实验, 实验中载体的利用率和数据嵌入量均有较大提高。实验结果如表2所示。

为评估本算法的稳健性, 结果如经过二次编码和加入高斯噪声后的提出的隐秘信息与原始信息相对比, 正确率仍然较高, 表明本算法具有较高的稳健性和较强的抗攻击能力。经过实验前后的同帧图像的对比可以发现, 在秘密信息的嵌入前后, 对载体信息的影响很小, 可以达到视觉不可见性的效果, 达到了预期的目的。攻击后秘密信息提取的正确率如表3所示。

表3 对本文算法进行攻击后数据提取的正确率

视频图像序列	进行二次编码后攻击	加入高斯噪声攻击
Mother-daughter	0.912	0.763
Tennis	0.905	0.742
Foreman	0.924	0.735
News	0.915	0.772

5 结语

本文提出的算法选择在利用 H.264 压缩编码的过程中进行秘密信息的嵌入。通过对秘密信息的交织技术处理, 可以达到对秘密信息的置乱; 利用卷积码具有较强纠错能力的特点, 可以有效地保护秘密信息, 从而达到不可见性和稳健性的特点; 同时利用不同相位, 代表不同的二进制序列, 大大提高了嵌入的容量。实验结果也证明: 在相同大小的数字视频载体中, 本文提出的方案能够有效地提高视频载体的利用率, 而且在视觉不可见性和秘密信息的稳健性方面有了更进一步的提升。

参考文献:

- [1] KUNG C H, JENG J H, LEE Y C. Video watermarking using motion vector[C]// CVGIP 2003: 16th IPPR Conference on Computer Vision, Graphics and Image Processing. 2003: 17-19.

分类的比较,如表4。

表4 数据集1的操作行为特征分类结果比较

操作行为特征数	TPR/%	TNR/%	准确率/%
500	96.05	90.79	93.42
8	94.74	94.74	94.74

从表4中可以看出,经过属性序约简后 TNR 和分类准确率有所提高,TPR 有所下降。

下面给出利用 API 短序列特征对数据集1的测试数据进行分类的比较,如表5。

表5 数据集1的API短序列特征分类结果比较

API 短序列特征数	TPR/%	TNR/%	准确率/%
500	97.37	100	98.68
6	98.68	100	99.34

从表5中可以看出,经过属性序约简后 TPR 和分类准确率得到了提高,TNR 保持不变。

下面给出利用操作行为特征对数据集2的测试数据进行分类的比较,如表6。

表6 数据集2的操作行为特征分类结果比较

操作行为特征数	TPR/%	TNR/%	准确率/%
500	95.56	85.56	90.56
10	94.44	94.44	94.44

从表6中可以看出,结果与表4基本相似,TNR 和分类准确率有所提高,TPR 有所下降。

下面给出利用 API 短序列特征对数据集2的测试数据进行分类的比较,如表7。

表7 数据集2的API短序列特征分类结果比较

API 短序列特征数	TPR/%	TNR/%	准确率/%
500	93.33	93.33	93.33
7	95.56	93.33	94.44

从表7中可以看出,结果与表5基本相似,TPR 和分类准确率有所提高,TNR 保持不变。

从上述结果中可以看出,利用属性序约简后的数量极少的特征进行分类的准确率比没有经过约简使用500个特征进行分类的准确率都要高,TNR 或有所提高或保持不变,而TPR 或有所提高或有所降低。虽然表4和表6的TPR 有所降低,但是分类准确率和 TNR 都有所提高,对于恶意代码检测而言,更倾向于降低误报率,即提高 TNR,因此符合检测的要求。同时,特征数目较少可以降低匹配复杂度,提高检测速度和响应能力。

6 结语

随着恶意代码数量的日益增多,智能化的代码危害性分析对恶意代码的检测和分析很有帮助。本文对基于调用踪迹的恶意代码自动分类进行了研究,重点对特征选择和约简进行研究,提出使用特征选择的信息来指导特征约简,使用属性序下的快速约简算法在较短的时间内获得较少数量的约简集。最后用实验验证了本文方法的有效性,使用约简集进行分类的效果较好。

参考文献:

- [1] 安天实验室. 安天实验室信息安全威胁综合报告[EB/OL]. [2010-07-12]. http://www.antiy.com/cn/security/2010/first_half_of_2010_the_Antiy_Laboratory_of_information_security_threats_roundup.pdf.
- [2] 安天实验室安全研究与应急处理中心. 对 Stuxnet 蠕虫攻击工业控制系统事件的综合报告[EB/OL]. [2010-09-02]. http://www.antiy.com/cn/security/2010/Report_On_the_Attacking_of_Worm_Struxnet_by_antiy_labs.htm.
- [3] SHABTAI A, MOSKOVITCH R, ELOVICI Y, *et al.* Detection of malicious code by applying machine learning classifiers on static features: A state-of-the-art survey [J]. Information Security Technology Report, 2009, 14(1): 16-29.
- [4] WILLIAMS C, HOLZ T, FREILING F. Toward automated dynamic malware analysis using cwsandbox [J]. IEEE Security and Privacy, 2007, 5(2): 32-39.
- [5] ANUBIS. Anubis: Analyzing unknown binaries [EB/OL]. [2010-09-16]. <http://anubis.iseclab.org>.
- [6] 刘赫. 文本分类中若干问题研究[D]. 长春: 吉林大学, 2009.
- [7] AHMED F, HAMEED H, SHAFIQ M, *et al.* Using spatio-temporal information in API calls with machine learning algorithms for malware detection and analysis [EB/OL]. [2009-08-24]. <http://nexginrc.org/nexginrcAdmin/PublicationsFiles/aisec09-faraz.pdf>.
- [8] 陈亮, 郑宁, 郭艳华, 等. 基于 Win32 API 的未知病毒检测[J]. 计算机应用, 2008, 28(11): 2829-2831.
- [9] 张波云. 计算机病毒智能检测技术研究[D]. 长沙: 国防科学技术大学, 2007.
- [10] 徐燕, 李锦涛, 王斌等. 文本分类中特征选择的约束研究[J]. 计算机研究与发展, 2008, 45(4): 596-602.
- [11] 胡峰, 王国胤. 属性序下的快速约简算法[J]. 计算机学报, 2007, 30(8): 1429-1435.
- [12] 徐章艳, 刘作鹏, 杨炳儒, 等. 一个复杂度为 $\max\{O(|C||U|), O(|C|^2|U||C|)\}$ 的快速属性约简算法[J]. 计算机学报, 2006, 29(3): 391-399.
- [13] 刘勇, 熊蓉, 褚健. Hash 快速属性约简算法[J]. 计算机学报, 2009, 32(8): 1493-1499.

(上接第962页)

- [2] 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.
- [3] XU CHANGYONG, PING XIJIAN, ZHANG TAO. Steganography in compressed video stream [C]// ICICIC'06. Washington, DC: IEEE, 2006: 269-272.
- [4] FANG DING-YU, CHANG LONG-WEN. Data hiding for digital video with phase of motion vector [C]// Proceedings of 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: 180-209.
- [6] 王新梅, 肖国镇. 纠错码——原理与方法[M]. 修订版. 西安: 西安电子科技大学出版社, 2006: 443-503.
- [7] 朱仲杰, 王玉儿, 蒋刚毅, 等. 基于自适应策略的稳健视频水印算法[J]. 计算机工程与应用, 2006, 36: 35-37.
- [8] HE XUANSEN, LUO ZHUN. A novel steganographic algorithm based on the motion vector phase [C]// International Conference on Computer Science and Software Engineering. Washington, DC: IEEE, 2008, 359: 822-825.