Journal of Computer Applications
计算机应用,2014,34(10):2840-2843
ISSN 1001-9081
CODEN JYIIDU
2014-10-10
http://www.joca.cn

文章编号:1001-9081(2014)10-2840-04
doi:10.11772/j.issn.1001-9081.2014.10.2840

基于运动矢量直方图不变的数字视频隐写算法

郭朝江*,张敏情,钮　可
(武警工程大学 电子技术系,西安 710086)
(*通信作者电子邮箱 1070960545@qq.com)

摘　要:针对现有基于运动矢量(MV)的数字视频隐写算法对载体直方图统计特性带来较大改变这一问题,提出一种基于运动矢量直方图不变的数字视频隐写算法。利用保持直方图数据映射方法,把秘密信息隐藏在视频运动矢量中;同时,利用数据匹配编码对嵌入之前的秘密信息进行编码处理,得到了与视频运动矢量统计特征基本匹配的数据流,使算法接近于信息论下的完美安全。实验结果表明:算法有效控制了运动矢量直方图的改变,同时码率的增加也被有效地控制在1%以内,隐写分析检出率平均下降了30%~50%。

关键词:视频隐写;运动矢量;直方图;匹配编码;数据映射
中图分类号:TP391　　**文献标志码**:A

Video steganography algorithm based on invariant histogram of motion vector

GUO Chaojiang*, ZHANG Minqing, NIU Ke
(*Department of Electronic Technology, Engineering University of Armed Police Force, Xi'an Shaanxi* 710086, *China*)

Abstract: To solve the problem that some video steganography algorithms based on Motion Vector (MV) change statistical features of histogram, a new video steganography algorithm based on keeping histogram of MV was proposed. In this paper, the secret information were hidden in video MV by using the data mapping of histogram. At the same time, a code-matching method was used to encode the secret information before being embedded, then the data stream would have the same statistical characteristics by MV, which made the scheme absolutely secure in theory. The experimental results show that: the change of histogram features is effectively controlled, the increment of bitrate is controlled in 1%, and the steganalysis detection rate is decreased by an average of 30% to 50%.

Key words: video steganography; Motion Vector (MV); histogram; matching coding; data mapping

0　引言

随着网络和通信技术的发展,信息安全问题变得日益突出,传统的加解密不能解决全部的信息安全问题。自20世纪90年代末,信息隐藏作为一门新兴的学科被提出来,在一定程度上解决和防止了数字化信息被篡改、伪造、盗版等问题。数字隐写作为信息隐藏的一个重要分支,在隐秘通信上起到了很重要的作用。

数字隐写的载体通常为文本、图像、音频和视频。一方面,视频相对于图像和音频具有更大的载体容量和更多的信息嵌入点;另一方面,以图像为载体的数字隐写的安全性也受到了越来越多的分析威胁。所以,近年来,数字视频隐写成为学者们研究的热点。

H.264/AVC[1]作为新一代的视频压缩编码标准,不仅具有更高的编码效率,而且还有良好的网络亲和性,已经取得了越来越广泛的应用。现有的针对H.264/AVC的数字隐写方法主要包括:基于运动矢量(Motion Vector, MV)进行信息嵌入[2-7]、基于量化后的整数变换系数[8]和基于帧内预测模式[9]进行信息嵌入。

运动矢量是在视频压缩过程中产生的,是视频数字隐写的重要嵌入点。基于运动矢量的数字隐写方案的优点如下:只需要对视频流进行部分解码,信息的嵌入和提取的复杂度相对较低;对视频质量的影响较小,尤其是对主观视频质量影响更小,这是由视频编码的整个过程决定的。

文献[2]根据人眼视觉特性,筛选出人眼较不敏感的运动矢量,计算其分量差以控制嵌入操作的位置,并在选定的运动矢量分量差中嵌入秘密信息。文献[3]通过预先定义的阈值选取幅值较大的运动矢量,根据相位角选取合适的运动分量,利用该分量在运动矢量中嵌入秘密信息,最后使用矩阵编码降低运动矢量的修改率。以上两种算法在获得较大的隐写容量的同时,算法对运动矢量直方图会造成较大变化;而运动矢量直方图特征是数字隐写分析的重要参考依据,因此,在进行运动矢量数字隐写时,必须考虑算法对运动矢量直方图带来的变化。

本文提出了一种新的基于运动矢量的数字视频隐写算法,算法利用一种能够达到预定输出直方图的随机数据映射方法,把秘密信息经过映射隐藏在视频运动矢量中;同时,在信息隐藏前利用Huffman有效码对秘密信息进行编码处理,经过Huffman编码处理的秘密信息具有与视频运动矢量相匹配的统计特征,使算法接近信息论上的完美安全。具体算法

收稿日期:2014-03-12;**修回日期**:2014-04-20。　**基金项目**:国家自然科学基金资助项目(61379152)。
作者简介:郭朝江(1989-),男,安徽淮北人,硕士研究生,主要研究方向:信息隐藏;　张敏情(1967-),女,陕西西安人,教授,博士,主要研究方向:信息安全、密码学;　钮可(1981-),男,浙江湖州人,硕士,主要研究方向:信息隐藏。

将在第 2 章介绍。

1　相关基础知识

1.1　保持载体直方图的数据映射方法

Eggers 等[10]指出:在没有信号失真和仅存在被动攻击的信道中,若秘密信息的嵌入过程不会改变载体的数字统计特性,那么该信道在理论上是一个不可检测的隐秘通道。本文在信息隐藏过程中采用了一种保持直方图的随机数据映射方法,用符号 F 表示该数据映射方法。

令 x 为定义在有限符号集 $X = \{x^1, x^2, \cdots, x^N\}$, $N = |X| < \infty$ $(x^1 < x^2 < \cdots < x^N)$ 上的离散随机变量,其直方图用 $h_x[i]$ 表示。令离散随机变量 y 表示 x 的映射结果,y 也是定义在有限符号集 $X = \{x^1, x^2, \cdots, x^N\}$ 上的离散随机变量,其直方图用 $h_y[j]$ 表示。

用 $i_n (i_n \in \{1,2,\cdots,N\})$ 表示一个输入信号 x_n 的符号上标,将 i_n 随机映射成一个连续随机变量 t,其分量表示为:$t_n = i_n - a_n$, a_n 是定义在 $[0,1)$ 上的均匀随机变量的一个值。可以得到 t 的概率密度分布函数必定与下面的函数成比例:

$$h_x(t) = \sum_{i=1}^{N} h_x[i]u(t + 1/2 - i) \tag{1}$$

其中:

$$u(v) = \begin{cases} 1, & -1/2 < v \leqslant 1/2 \\ 0, & \text{其他} \end{cases}$$

为了获得直方图 $h_x[i]$ 和 $h_y[j]$ 的积分,引入两个函数:

$$\begin{cases} h_x(t) = \sum_{i=1}^{N} h_x[i]r(t - i) \\ h_y(t) = \sum_{j=1}^{N} h_y[j]r(t - j) \end{cases} \tag{2}$$

其中:$r(t)$ 表示单位脉冲函数。

如果要保证数据映射的结果 y 满足预定的直方图 $h_y[j]$,必须使:

$$\begin{cases} \int_0^1 h_y(\tau)\mathrm{d}\tau = \int_0^1 h_x(\tau)\mathrm{d}\tau \\ \int_{j-1}^{j} h_y(\tau)\mathrm{d}\tau = \int_{j-1}^{j} h_x(\tau)\mathrm{d}\tau \end{cases} ; \forall j \in \{2,3,\cdots,N-1\} \tag{3}$$

解上述积分方程,可以得到集合 $T = \{t_1, t_2, \cdots, t_{N-1}\}$。以 T 为阈值定义量化器 Q_t:

$$Q_t = \begin{cases} x^1, & t \leqslant t_1 \\ x^j, & t_{j-1} < t \leqslant t_j; \ \forall j \in \{2,3,\cdots,N-1\} \\ x^N, & t_{N-1} < t \end{cases} \tag{4}$$

则量化器 Q_t 的输出 $y_n = Q_t(t_n) = Q_t(i_n - a_n)$ 即为本文所期望的输入数据 x_n 的映射结果。

1.2　数据匹配编码

Huffman 有效码[11]是对给定信源的信源空间和规定的码符号集,合理利用信源的统计特性构造的单义可译码,因此可以利用 Huffman 有效编码对嵌入的数据进行预处理。处理过程如图 1 所示。首先根据所期望的信源符号“0”和“1”的出现概率设计 Huffman 有效码;然后使用所设计的 Huffman 有效码对数据流进行编码处理。

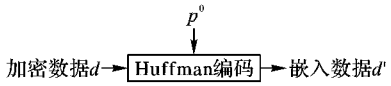


图 1　信息匹配编码示意图

其中:d 表示处理前的数据流,通常 $p(d = 0) \approx p(d = 1) \approx 0.5$;用 d' 表示处理后的数据流,要求满足 $P(d' = 0) = P^0$, P^0 是给定信源空间偶数值出现的概率。则具体步骤为:

1) 设计 Huffman 有效码,使信源符号“0”和“1”的出现概率为 $P(\text{符号} = 0) = p^0$, $P(\text{符号} = 1) = 1 - p^0$。

为了使所构造的 Huffman 有效码更好地满足信道统计特征,即:$P(\text{符号} = 0) = p^0$,本文将几个信源符号组合在一起,并且符号组越长效果越好,从而可以得到长度不同的编码。例如选择双符号组合,赋值 $p^0 = 0.7$,则有:

00 – 1

01 – 01

10 – 000

11 – 001

2) 用上述设计的 Huffman 有效码解码数据流 d,即:

1 – 00

01 – 01

000 – 10

001 – 11

当数据流 d 达到一定长度时,在统计意义上,处理后得到的数据流 d' 必然满足 $P(d' = 0) = P^0$。

1.3　数据嵌入方法

在进行数据嵌入时,首先提取视频运动矢量,把大于设定的阈值 $|\boldsymbol{MV}|$ 的幅值集合 Y 按奇偶性分成互不相交的两个集合 $Y_0 = \{\text{偶幅值}\}$ 和 $Y_1 = \{\text{奇幅值}\}$。

运用 1.1 节提到的数据映射方法,定义两个数据映射:

$F_0: Y \to Y_0$, $F_1: Y \to Y_1$

令 $\boldsymbol{c}_n$ 表示原始视频第 n 个运动矢量,$\boldsymbol{s}_n$ 表示载密视频的第 n 个运动矢量,使用经 1.2 节调制的秘密数据流 d' 控制两个映射 F_0 和 F_1 之间的转换,从而实现在载体运动矢量中嵌入秘密信息的目的,具体过程如图 2 所示。

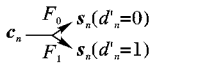


图 2　数据嵌入方法

2　算法设计

2.1　嵌入规则

信息的嵌入过程可以分为 5 步:

1) 数据加密。算法采用较为成熟的对称加密算法数据加密标准(Data Encryption Standard, DES),将待隐藏的秘密信息 m 加密成二进制数据流 d。

2) 统计载体运动矢量特性。以一组图像组(Group Of Pictures, GOP)为单位,提取 P 帧和 B 帧的运动矢量,计算运动矢量的幅值,统计隐秘视频载体 C 的运动矢量大于设定的阈值 $|\boldsymbol{MV}|$ 的偶幅值出现的概率并记为 p^0。

3) 数据匹配编码。使用 1.2 节中描述的方法对数据流 d 进行信道特性匹配编码,得到与载体运动矢量数字特性基本

相匹配的数据流 d',计算数据流长度并记为 L。

4)数据嵌入。采用 1.1 和 1.3 节中描述的数据映射方法对秘密信息进行嵌入,其中最开始的 16 个载体运动矢量嵌入 p^0,接着的 32 个载体运动矢量嵌入 L,然后的载体运动矢量依次嵌入数据流 d',形成了嵌入秘密信息的视频运动矢量。

5)将嵌入秘密信息的运动矢量进行 H.264/AVC 编码传输,完成信息的嵌入。

2.2 提取规则

信息的提取过程为:

1)接收方从接收到的 H.264/AVC 视频信息提取运动矢量最低有效位,其中最开始 16 位是 p^0,紧接着 32 位是 L,然后是隐藏的 L 位嵌入数据流 d'。

2)对提取得到的 L 位嵌入数据流 d' 进行数据匹配解码,得到数据流 d。

3)接收方运用密钥对数据流 d 进行解密,最终获得传输的秘密信息 m。

2.3 算法分析

2.3.1 算法安全性分析

在隐藏信息嵌入到运动矢量之前,用对称加密算法 DES 对信息进行加密,确保了秘密信息的不可见性。同时,由于视频运动矢量的幅值普遍较小,在其中嵌入信息会造成比较严重的视觉失真,因此,事先设定阈值 $|\boldsymbol{MV}|$,使得运动矢量幅值大于 $|\boldsymbol{MV}|$ 的才会进行信息的隐藏,确保算法不会对视频信息造成明显的主观上的失真。利用 Eggers 等[10] 提出的保持直方图数据映射的方法,通过秘密信息控制原始运动矢量与两个映射之间的转换,使得嵌入前后运动矢量的直方图保持了较高维数的数字特征,并且利用 Huffman 有效码对加密后的信息进行编码,得到了与载体运动矢量统计特征相匹配的数据流,使得方案在仅存在被动攻击的情况下信息论意义上是绝对安全的。下面理论证明算法的安全性。

2.3.2 算法安全性证明

根据 1.1 节和 1.3 节中设计的数据嵌入规则,结合 Cachin[12] 提出的隐秘通信系统安全性意义,进行算法安全性证明。

隐秘载体 s 的条件概率密度函数为:

$$p_s[s \mid d' = i] = \begin{cases} \dfrac{p_c[s]}{P(c \in Y_i)}, & s \in Y_i \\ 0, & s \notin Y_i \end{cases}; \ \forall i \in \{0,1\} \tag{5}$$

由式(5)可以推出隐秘视频载体 s 的概率密度函数为:

$$p_s[s] = P(d'=0)p_s[s \mid d'=0] + P(d'=1)p_s[s \mid d'=1] = \begin{cases} \dfrac{P(d'=0)}{P(c \in Y_0)} p_c[s], & s \in Y_0 \\ \dfrac{P(d'=1)}{P(c \in Y_1)} p_c[s], & s \in Y_1 \end{cases} \tag{6}$$

经过加密的信息,一般有下式成立:

$$P(d=0) \approx P(d=1) = 0.5 \tag{7}$$

而经过 Huffman 有效码解码的数据流满足:

$$P(d'=0) \approx p^0 \tag{8}$$

根据定义可以得到:

$$P(d'=0) \approx P(c \in Y_0) \tag{9}$$

也就是:

$$P(d'=1) \approx P(c \in Y_1) \tag{10}$$

由式(6) ~ (10)可得出:

$$p_s[s] = \begin{cases} \dfrac{P(c \in Y_0)}{P(c \in Y_0)} p_c[s], & s \in Y_0 \\ \dfrac{P(c \in Y_1)}{P(c \in Y_1)} p_c[s], & s \in Y_1 \end{cases} \tag{11}$$

由式(11)可以得到:

$$p_s[s] = p_c[s] \tag{12}$$

结合式(12)从相对熵的角度出发,可以得到:

$$D(p_c \| p_s) = \sum p_c \operatorname{lb} \frac{p_c}{p_s} = 0 \tag{13}$$

根据 Cachin[12] 的观点,可以得到本文描述的算法在信息论意义上是接近于绝对安全的。

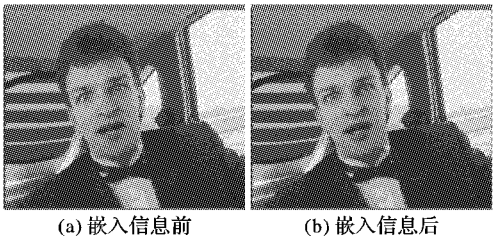
3 实验结果

本文实验所用电脑配置为 Core i3-3217u CPU (1.8 GHz),4.0 GB RAM,在 X264 编码器平台上使用VC++ 6.0 进行仿真实验。

3.1 运动矢量直方图变化

实验中选取标准的 YUV 格式序列 Carphone(300 帧 176×144)作为标准测试序列。设定 $|\boldsymbol{MV}|=6$,用本文算法进行秘密信息的嵌入,实验结果如图 3 ~ 5 所示。

由图 3 可以看出,测试视频在信息嵌入前后并未发生明显改变。人眼察觉不出嵌入信息的存在,说明算法能够达到主观的视觉不可见性。



(a) 嵌入信息前 (b) 嵌入信息后

图 3 视频帧隐写前后对比

图 4 和图 5 中横轴表示运动矢量的幅值,纵轴表示对应运动矢量幅值的个数,实验中,carphone_qcif(176×144)运动矢量共 16574 个。可以看出,绝大部分运动矢量的幅值均为 0,算法未对幅值较小的运动矢量进行改变;秘密信息嵌入前后,运动矢量直方图未发生明显改变,能够实现算法抵抗针对运动矢量直方图特征分析的攻击。

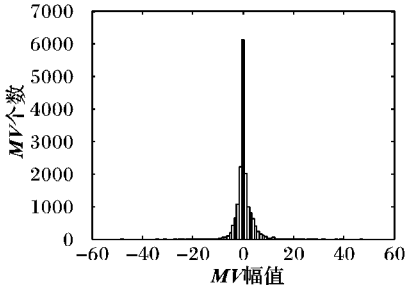


图 4 信息嵌入前载体运动矢量直方图

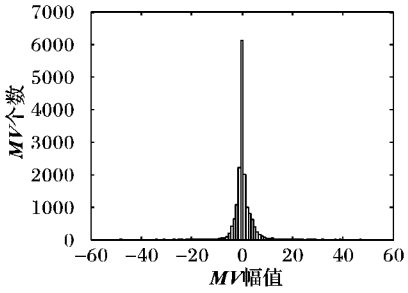


图 5　信息嵌入后载体运动矢量直方图

3.2　信息嵌入前后码率变化

实验中,选取标准的 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。对每一组视频,采用本文的算法嵌入随机生成序列,对幅值大于事先设定的阈值($|MV|=6$)的运动矢量进行满嵌。实验结果如表 1 所示。

表 1　信息嵌入前后码率的变化

视频	信息嵌入前信息容量/kb	信息嵌入后信息容量/kb	码率变化/%
Mother-daughter	44 550	44 960	0.92
Tennis	3 207	3 241	1.05
Foreman	2 331	2 351	0.87
News	1 603	1 618	0.94

从表 1 不难看出,信息嵌入前后,视频的码率虽然有所增加,但是总体上讲,码率的增加都基本控制在 1% 以内,对于传输或者存储不会造成负担。

3.3　隐写分析检测率

根据 Su 等[13]提出的质心在隐写前后会衰减的特性,计算待检测视频中质心混叠程度作为特征向量,最后使用比较成熟的支持向量机(Support Vector Machine, SVM)作为分类器对特征向量进行检测分类,利用该检测方法对文献[2 - 3]算法和本文隐写算法进行检测,实验结果如表 2 所示。其中 *TP* 表示检测算法对隐秘视频正确的检测率。

文献[14]通过运动补偿技术恢复出当前运动矢量的估计值,提取估计值同待检测矢量间相关性的统计特征,采取分类判别的方式对隐藏信息的运动矢量进行检测。利用该检测方法对文献[2 - 3]算法和本文隐写算法进行检测,实验结果如表 2 所示。

本文实验设定($|MV|=6$),实验对象为 16 个 CIF 视频序列:每个视频序列均采用 4:2:0 的 YUV 格式。考虑到待检测视频序列的视频长度不同,实验中随机选取每个视频 30 帧无重复的子序列作为实验数据。

表 2　隐写分析的实验平均结果

检测算法	隐写算法	检测隐秘视频个数	*TP* /%
文献[13]检测算法	文献[2]算法	12	75.00
	文献[3]算法	10	62.50
	本文算法	4	25.00
文献[14]检测算法	文献[2]算法	12	75.00
	文献[3]算法	7	43.75
	本文算法	2	12.50

根据表 2 可知,本文算法相比文献[2]和文献[3]算法,在针对运动矢量的隐写分析检测下,隐写分析检出率平均下降了 30% ~ 50%,安全性有大幅提高。

参考文献:

[1] BI H. A new generation of video compression coding standard - H.264/AVC [M]. Beijing: Posts & Telecom Press, 2005: 133 - 208. (毕厚杰. 新一代视频压缩编码标准: H.264/AVC[M]. 北京: 人民邮电出版社, 2005: 133 - 208.)

[2] WANG J, ZHANG M, YANG X. Video steganography algorithm based on difference of motion vector components [J]. Computer Engineering, 2011, 37(23): 135 - 137. (王珏, 张敏情, 杨晓元. 基于运动矢量分量差的视频隐写算法[J]. 计算机工程, 2011, 37(23): 135 - 137.)

[3] ZHAO L, YANG X, NIU K, *et al*. Video steganographic method with low modification rate [J]. Computer Engineering, 2011, 37(20): 130 - 132. (赵李懿, 杨晓元, 钮可, 等. 一种低修改率的视频隐写方法[J]. 计算机工程, 2011, 37(20): 130 - 132.)

[4] FANG D, CHANG L. Data hiding for digital video with phase of motion vector [C]// Proceedings of the 2006 IEEE International Symposium on Circuits and Systems. Piscataway: IEEE Press, 2006: 4.

[5] WANG P, ZHENG Z, LI L. A video watermarking scheme based on motion vectors and mode selection [C]// Proceedings of the 2008 International Conference on Computer Science and Software Engineering. Piscataway: IEEE Press, 2008, 5: 233 - 237.

[6] ALY H A. Data hiding in motion vectors of compressed video based on their associated prediction error [J]. IEEE Transactions on Information Forensics and Security, 2011, 6(1): 14 - 18.

[7] CAO Y, ZHAO X, FENG D, *et al*. Video steganography with perturbed motion estimation [C]// Proceedings of the 13th International Conference on Information Hiding. Berlin: Springer-Verlag, 2011: 193 - 207.

[8] GOLIKERI A, NASIOPOULOS P, WANG J. An improved scalar quantization-based digital video watermarking scheme for H.264/AVC [C]// Proceedings of the 2006 IEEE International Symposium on Circuits and Systems. Piscataway: IEEE Press, 2006: 5.

[9] HU Y, ZHANG C, SU Y. Information hiding for H.264/AVC [J]. Acta Electronica Sinica, 2008, 36(4): 690 - 694. (胡洋, 张春田, 苏育挺. 基于 H.264/AVC 的视频信息隐藏算法[J]. 电子学报, 2008, 36(4): 690 - 694.)

[10] EGGERS J J, BÄEUML R, GIROD B. A communications approach to image steganography [EB/OL]. [2013-12-26]. http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=8F3BB4F4F626B0004F25E912460EBDE8?doi=10.1.1.15.7094&rep=rep1&type=pdf.

[11] LIU C. Researeh on steganographic theory and techniques [D]. Nanjing: Nanjing University of Science and Technology, 2004. (刘春庆. 隐秘通信理论与技术研究[D]. 南京: 南京理工大学, 2004.)

[12] CACHIN C. An information-theoretic model for steganography [C]// Proceedings of the 2nd International Workshop on Information Hiding. Berlin: Springer-Verlag, 1998: 306 - 318.

[13] SU Y, ZHANG C, ZHANG C. A video steganalytic algorithm against motion-vector-based steganography [J]. Signal Processing, 2011, 91(8): 1901 - 1909.

[14] CAO Y, ZAHO X, FENG D. Video steganalysis exploiting motion vector reversion-based features [J]. IEEE Signal Processing Letters, 2012, 19(1): 35 - 38.