

基于H.264标准的视频混沌密写算法

汪 波, 冯久超

(华南理工大学 电子与信息学院, 广州 510641)

摘要: 基于目前最新的视频编码标准H.264, 运用混沌加密和混沌密写, 提出一种视频混沌密写算法。采用标准视频序列进行了仿真, 并分析了算法的性能。结果表明: 该算法不仅能快速和有效地进行密写, 而且解码后视频序列的视觉效果和峰值信噪比(PSNR)基本上不受密写影响。

关键词: 通信技术; H.264标准; 视频; 混沌密写; 混沌加密

中图分类号: TN918.7 **文献标识码:** A **文章编号:** 1671-5497(2008)04-0960-06

Chaos steganography algorithm for video sequence based on H.264

WANG Bo, FENG Jiu-chao

(School of Electronic and Information Engineering, South China University of Technology, Guangzhou 510641, China)

Abstract: On the basis of the recently proposed video coding standard H.264, a chaos steganography algorithm with chaos encryption and chaos steganography was presented. Performance analysis of the proposed algorithm was given by using standard video sequences. Simulation results indicate that this steganography algorithm can be fast and effectively implemented, and visual effect and peak signal to noise ratio (PSNR) of the video sequences are almost not affected after decoding.

Key words: communication; H.264 standard; video; chaos-steganography; chaos-encryption

目前, 随着大量无线产品的大众化以及用户对无线产品潜在安全威胁的担心, 数字通信的安全性越来越受到关注, 因此信息保护问题对现代加密和密写技术提出了一个新的挑战^[1]。密写(Steganography)是一种将秘密信息安全发送到目的地而不引起攻击者注意的技术^[2]。密写技术以数字媒体作为载体, 运用强大的计算机运算能力和信号处理技术来隐藏信息并将载密媒体发布到网络上。文献[3]表明“每出现一种巧妙的多媒体信息隐藏的方法, 都会有一种同等巧妙的检测

或揭示秘密信息方法出现”, 虽然信息隐藏检测方面国内外已有许多学者在研究, 但要在海量的可从网络上下载的多媒体数据中检测出隐藏信息仍然是非常困难的^[4]。混沌加密原理是将混沌映射迭代产生的混沌序列作为加密变换的一个因子序列^[5]。混沌信号对初值非常敏感, 具有类随机特性, 利用这些特性可以实现对明文的加密。

目前, 在混沌密写研究方面, 王海春^[6]将混沌应用于密写中, 提出用混沌来控制密写。在视频密写研究方面主要有两个方向: 用于隐秘通信和

收稿日期: 2007-02-15.

基金项目: 国家自然科学基金项目(60572025); 教育部新世纪优秀人才基金项目(NCET-04-0813, 重点项目: 105137); 广东省自然科学基金项目(04205783, 07006496).

作者简介: 汪波(1984-), 男, 硕士研究生。研究方向: 图像和视频信号分析与处理。E-mail: wb901c@21cn.com

通信作者: 冯久超(1964-), 男, 教授, 博士生导师。研究方向: 数字信号处理, 数字通信, 非线性动力学及混沌理论与应用。E-mail: fengjc@scut.edu.cn

纠错。对于前者, Xu 等^[7]将信息嵌入到 MPEG 视频压缩编码数据的运动向量中, Westfeld 等^[8]将信息嵌入到 H.261 视频编码数据的 DCT 变换系数中;而对后者, Robie 等^[9-10]将密写运用于 MPEG-2 中对视频码流进行误码检测和纠错。目前视频编码标准发展迅速,如 MPEG-1, MPEG-2, MPEG-4, H.261, H.263 及 H.264。对不同的标准,应根据它们自身的不同特点设计出不同的密写算法^[11]。目前,作者还没有见到结合了 H.264 标准并运用混沌密写对视频数据实施密写的文献报道。为此,作者以 H.264 标准为基础,充分考虑 H.264 和混沌的特点,综合混沌加密和混沌密写,提出和实现一种将密文嵌入到经整数变换与量化后的数据中的视频混沌密写算法。

1 算法框图

根据算法整体框架(见图 1),隐秘通信过程

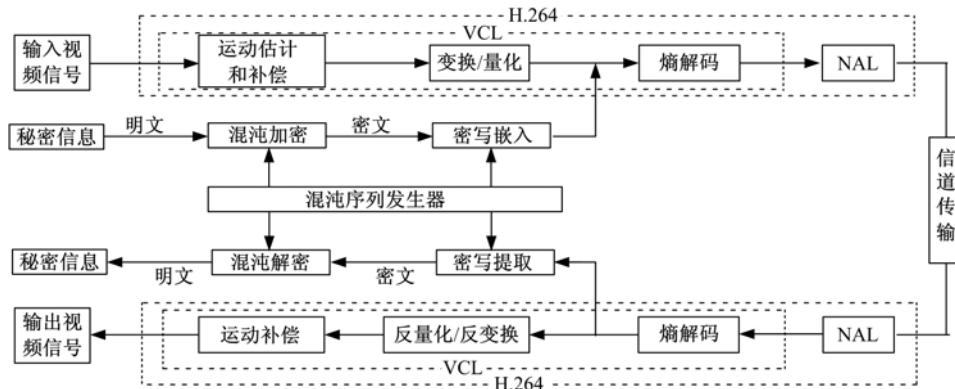


图 1 基于 H.264 标准的视频混沌密写方案

Fig. 1 Video chaos-steganography scheme based on H.264 standard

2 加密方案

加密为第 1 道防线,其后的密写为第 2 道防线,监听者在无密钥情况下很难从载体数据中提取密文,也就更难提取明文了,具体方案如下。

(1)由 C 产生混沌序列 S_k ,用规一化函数 f 使 $l_k = f(S_k)$, $0 \leq l_k \leq 255$ 。

(2)每次加密的明文规定长度为 M 字节,超过 M 字节则进行分段,每段 M 字节,不足的后面补 0。

(3)每次用于加密的序列 $L_i = [l_{i \times M+1}, l_{i \times M+2}, \dots, l_{i \times M+M}]$, $i=0,1,\dots$

(4)加密过程为: $c = EC(m, L_i) = m \oplus L_i$, \oplus 为按位异或运算。

(5)解密过程为: $m = DEC(c, L_i) = c \oplus L_i$ 。

可描述为:双方根据建立连接时获得的密钥初始化混沌序列发生器 C,发送方从 C 中取得一加密序列 L_i ($i=1,2,\dots$) 和一个控制序列 G_k ($k=1,2,\dots$),用加密算法 $EC(\cdot)$ 将秘密信息(明文) m 加密为密文 c ,再用密写算法 $ES(\cdot)$ 将 c 嵌入到视频序列中,得到载密的视频序列 d ,最后将 d 通过信道传输到接收方。接收方也从 C 中取得对应的解密序列 L_i 和控制序列 G_k ,用密写提取算法 $DES(\cdot)$ 从载密视频序列 d 中提取出密文 c ,用解密算法 $DEC(\cdot)$ 获得明文 m 。该过程用公式表示如下

发送过程

$$c = EC(m, L_i) \quad (1)$$

$$d = ES(c, G_k) \quad (2)$$

接收过程

$$c = DES(d, G_k) \quad (3)$$

$$m = DEC(c, L_i) \quad (4)$$

混沌序列 S_k 由 logistic 映射产生,动力学方程如式(5)所示,采用的规一化方法如式(6)所示

$$S_{k+1} = \alpha S_k (1 - S_k) \quad (5)$$

$$l_k = f(S_k) = (S_k \times 10^\beta) \bmod 256 \quad (6)$$

式中: α 为混沌映射的系统参数; β 为取长因子(例如 $\beta=6$, 则 $S_k \times 10^\beta$ 即为取 S_k 小数点后 6 位数),这里的 α, β, M 均可作为密钥。

3 密写方案

在 H.264 标准中,主要采用 4×4 的整数变换,在亮度的 16×16 Intra 模式中除了采用 4×4 的整数变换外,还抽出 4×4 DC 系数进行二次变换,在 8×8 宏块中,也抽出 2×2 DC 系数进行二次变换,这是 H.264 标准中编码部分的特点;H.264 中的量化为标量量化,但采用的是可变步

长量化,变化幅度控制在 12.5% 左右^[12]。H.264 编码器的基本结构如图 2 所示。

密写嵌入可实施在量化后的 AC 系数或 DC 系数上。而实施在 DC 系数上时要做特殊处

理^[13],通常在非零 AC 系数上密写,另外考虑新标准的特点,对于 DC 系数和二次变换系数均不实施密写,不改变环内用于预测的数据,密写嵌入实施在编码器的环外。

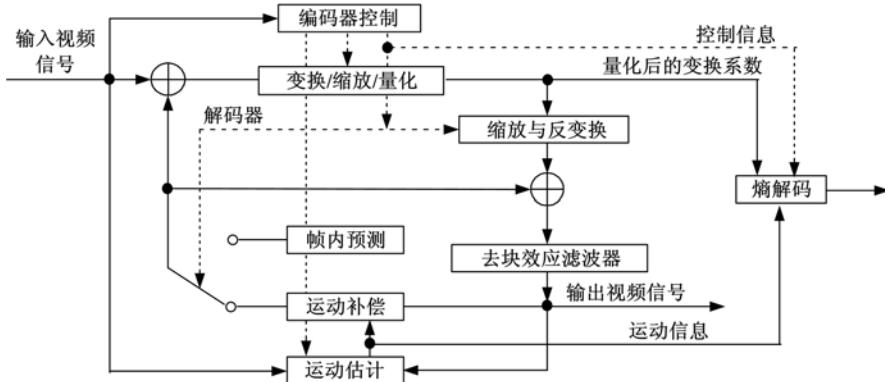


图 2 H.264 编码器的基本结构

Fig. 2 Basic structure of H.264 coder

3.1 密写算法

简单最低有效位(Least significant bit, LSB)密写直接比较密写数据与载体的 LSB,不同则修改,而 F5 算法^[14]用更多载体 LSB 承载信息,以降低载体数据利用率来换取嵌入效率。作者受 F5 算法启发,在嵌入时增加控制位并用混沌序列控制其位置。具体密写算法如下:

(1) 设长度为 N 的嵌入比特流为 b_1, b_2, \dots, b_N , 其中 $b_i = 0$ 或 1 ($i = 1, 2, \dots, N$); 载体数据的个数为 $N+1$, 设其 LSB 为 d_0, d_1, \dots, d_N , 其中 $d_i = 0$ 或 1 ($i = 0, 1, \dots, N$)。

(2) 设控制密写嵌入的混沌序列为 G_k ($k = 1, 2, \dots$)。

(3) 从 d_0, d_1, \dots, d_N 中选取一个控制位, 设所选 LSB 的下标为 $c b_k$, $c b_k$ 由下式计算

$$c b_k = \text{round}[G_k \times (N+1)] \quad (7)$$

式中: $\text{round}[\cdot]$ 为四舍五入取整运算。由于 $G_k \in (0, 1)$, 所以 $c b_k \in [0, N]$ 。

(4) 除控制位外, 其余 N 个 LSB 与要嵌入的比特按顺序依次对应, 设这 N 个 LSB 与要嵌入的比特相同的个数为 n, 修改规则如下: ① 当 $n > N - n$ 时, 置 d_{cb_k} 为 0, 进行直接嵌入; ② 当 $n < N - n$ 时, 置 d_{cb_k} 为 1, 将比特取反嵌入; ③ 当 $n = N - n$ 时, 根据原始的 d_{cb_k} 值决定是直接嵌入还是取反嵌入。

提取写过程如下:

(1) 首先接收方据 C 取得 G_k , 按式(7)得到。

(2) 取出 d_{cb_k} , 若 d_{cb_k} 为 1, 则将取得的 LSB 取反则为所得的值; 若 d_{cb_k} 为 0, 则所取得的 LSB 即为所得的值。

3.2 性能分析

设载体的 LSB 值是随机的, 同时秘密信息比特经加密扰乱后也是随机的, 设随机变量 X 为修改 LSB 的个数, 值可为 $0, 1, \dots, K$, 概率分布为 $P\{X=i\} = p_i$, R 为载体数据利用率, E 为嵌入效率, 表示每个 LSB 修改可以嵌入的平均比特数, D 为嵌入 N 比特信息所用载体数据个数, 则有如下的关系式。

随机变量 X 的数学期望为

$$E(X) = \sum_{i=0}^K i \times p_i \quad (8)$$

载体数据利用率为

$$R = N/D \quad (9)$$

嵌入效率为

$$E = N/E(X) \quad (10)$$

(1) 对简单 LSB 密写, 嵌入 N 比特信息时, X 的值可为 $0, 1, \dots, N$, 其概率分布为

$$\begin{aligned} P\{X=i\} &= p_i = C_N^i / 2^N \\ i &= 0, 1, \dots, N \end{aligned} \quad (11)$$

将式(11)代入式(8)得随机变量 X 的数学期望

$$\begin{aligned} E(X) &= \sum_{i=0}^N i \times p_i = \sum_{i=0}^N i \times C_N^i / 2^N = N/2 \\ (12) \end{aligned}$$

嵌入 N 比特秘密信息需要 N 个载体数据, $D = N$, 所以载体数据利用率为

$$R = N/D = N/N = 1 \quad (13)$$

将式(12)代入式(10)得嵌入效率

$$E = N/E(X) = 2 \quad (14)$$

(2)对F5密写,嵌入N比特信息最多只需修改1个LSB,X的取值为0或1,其概率分布为 $P\{X=0\}=1/2^N$, $P\{X=1\}=(2^N-1)/2^N$,则随机变量X的数学期望为

$$E(X) = 0 \times P\{X=0\} + 1 \times P\{X=1\} = (2^N-1)/2^N \quad (15)$$

其中嵌入N比特秘密信息需要 2^N-1 个载体数据, $D=2^N-1$,则载体数据利用率为

$$R = N/D = N/(2^N-1) \quad (16)$$

将式(15)代入式(10)得嵌入效率

$$E = N/E(X) = N \times 2^N/(2^N-1) \quad (17)$$

(3)本文方法修改信息位的个数为 $\min(n, N-n)$,n为载体LSB与嵌入比特依次对应相同的个数,另外考虑控制位,X的取值分两种情况:当N为奇数时,X的值可为 $0,1,\dots,(N+1)/2$,设 $j=N-n$,则当 $j \leq (N-1)/2$ 时,修改个数为j或 $j+1$,其概率均为 $(C_N^j/2^N) \times 1/2$,当 $j > (N-1)/2$ 时,修改个数的取值及其概率与 $j \leq (N-1)/2$ 时是对称的,得随机变量X的概率分布如下

$$P\{X=i\} = p_i = \begin{cases} C_N^0/2^N, & i=0 \\ (C_N^{i-1} + C_N^i)/2^N, & i=1,2,\dots,(N-1)/2 \\ C_N^{(N-1)/2}/2^N, & i=(N+1)/2 \end{cases} \quad (18)$$

同理,当N为偶数时,X可能的取值为 $0,1,\dots,N/2$,概率分布为

$$\begin{cases} C_N^0/2^N, & i=0 \\ (C_N^{i-1} + C_N^i)/2^N, & i=1,2,\dots,N/2 \end{cases} \quad (19)$$

当N为奇数时,将式(18)代入式(8)得

$$E(X) = \sum_0^{(N+1)/2} i \times p_i = \frac{N+1}{2} C_N^{(N-1)/2}/2^N + \sum_1^{(N-1)/2} i \times (C_N^{i-1} + C_N^i)/2^N = \frac{N+1}{2} \left[1 - \frac{C_N^{(N-1)/2}}{2^N} \right] \quad (20)$$

同理,当N为偶数时,将式(19)代入式(8)得

$$E(X) = \frac{N+1}{2} \left[1 - \frac{C_N^{N/2}}{2^N} \right] \quad (21)$$

综合式(20)和式(21)得随机变量X的数学期望

$$E(X) = \begin{cases} \sum_0^{(N+1)/2} i \times p_i = \frac{N+1}{2} (1 - C_N^{(N-1)/2}/2^N), & N \text{为奇数} \\ \sum_0^{N/2} i \times p_i = \frac{N+1}{2} (1 - C_N^{N/2}/2^N), & N \text{为偶数} \end{cases} \quad (22)$$

在本文的算法中增加了一个控制位,所以 $D=N+1$,从而载体数据利用率为

$$R = N/D = N/(N+1) \quad (23)$$

将式(22)代入式(10)得嵌入效率

$$E = \frac{N}{E(X)} = \begin{cases} N / \left[\frac{N+1}{2} (1 - C_N^{(N-1)/2}/2^N) \right], & N \text{为奇数} \\ N / \left[\frac{N+1}{2} (1 - C_N^{N/2}/2^N) \right], & N \text{为偶数} \end{cases} \quad (24)$$

根据以上分析,平均修改个数 $E(X)$ 、载体数据利用率为 R 和嵌入效率 E 的对比如图3所示。

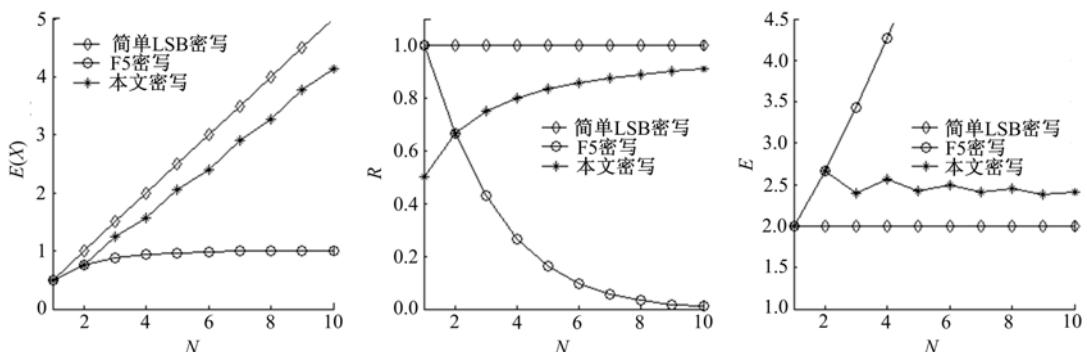


图3 算法性能对比

Fig. 3 Comparison of algorithm performance

由图3可知,本文算法虽然增加了一个控制位,数据利用率稍有下降,但嵌入效率提高了近21%,且算法过程简单快速。从安全角度来看,在信息位中插入控制位并且位置由混沌序列控制,使监听者在无密钥情况下获取密文更加困难。

4 仿真结果与分析

用3个QCIF格式(图像尺寸为 176×144)标

准视频序列对算法进行仿真实验,PC配置为:3.0 GHz P4处理器,512 MB RAM。观察密写后在编码端实施加密和密写的时间开销、视觉效果和峰值信噪比PSNR的变化情况。

首先观察视觉效果变化情况。向非零AC系数嵌入256字节信息,嵌入前后I帧解码图像序列如图4所示。从实验结果可以看出,密写前后视频图像的视觉效果无明显变化。



图4 嵌入前后的解码器输出帧图像

Fig. 4 Output frame images of decoder before and after embedding

其次,分析YUV分量PSNR的变化。因为改变了部分量化后的AC系数,量化步长相同时,PSNR主要受嵌入长度影响,此时各序列I帧的PSNR如表1所示。易知,嵌入256字节信息,PSNR平均变化不到0.1 dB,密写对PSNR的影响非常小。

改变量化步长时PSNR主要受量化步长改

表1 嵌入前后PSNR的变化(QP=28)

Table 1 Change of PSNR before and after embedding

参数	密写前各分量PSNR			密写后各分量PSNR		
	Y	U	V	Y	U	V
Foreman	37.3757	41.2599	42.8501	37.3704	41.1425	42.7417
Highway	38.9410	38.1778	39.0677	38.9688	38.1778	39.0677
Container	37.3914	40.9818	40.9244	37.4155	40.9818	40.9284

变量影响,Y分量PSNR随量化参数变化如表2所示,从表2中可看出,密写对各序列I帧PSNR的影响相对量化步长改变对PSNR的影响要小得多。

表2 不同QP对Y分量PSNR的影响

Table 2 PSNR of Y component effected by different QP

参数	峰值信噪比PSNR/dB					
	QP=26	QP=27	QP=28	QP=29	QP=30	QP=31
Foreman	38.7356	37.9762	37.3757	36.6384	35.8568	35.2971
Highway	40.0370	39.4099	38.9410	38.3154	37.7132	37.2257
Container	38.7643	37.9958	37.3914	36.5828	35.8095	35.3312

最后,分析算法时间开销,即分析当需要改变LSB个数接近最大值 $1+N/2$ 时的时间开销及与嵌入长度的关系。嵌入不同长度秘密信息的最大

时间开销如表 3 所示。从中可看出,时间开销均为微秒级,当嵌入长度超过 4 kB 时,时间开销才会达到毫秒级,而这个长度作为段长已经足够了。对于实时单帧编码时间开销为毫秒级,其影响可以忽略。

表 3 算法时间开销

Table 3 Time spending of algorithm

嵌入信息长度/byte	实际修改个数/bit	时间开销/μm
128	510	31
256	1023	61
512	2023	122
1024	4055	242
4096	16296	977

同时还可以看出,最大时间开销与嵌入长度基本成正比,从而当嵌入不同长度的秘密信息时,可以据此对最大时间开销进行估计,在实际应用中可以做为帧率设定的参考。

5 结束语

以目前最新的视频编码标准 H.264 为基础,提出并实现了一种基于混沌的视频密写方法。通过用标准视频序列进行仿真和理论分析表明,这种算法不仅能快速有效地密写,而且解码后视频序列的视觉效果和信噪比基本不受密写影响。该算法可以直接应用于实际基于 H.264 标准的视频通信系统中进行隐秘通信。

参考文献:

- [1] Satish K, Jayakar T, Tobin C, et al. Chaos based spread spectrum image steganography [J]. IEEE Transactions on Consumer Electronics, 2004, 50(2): 587-590.
- [2] Petitcolas F A P, Aderson R J, Kuhn M G. Information hiding——a survey [J]. Proc of the IEEE, 1999, 87(7): 1062-1078.
- [3] Wang H, Wang S. Cyber warfare: steganography vs. steganalysis [J]. Communication of ACM, 2004, 47(10): 76-82.
- [4] Provos N, Honeyman P. Detecting steganographic content on the internet [R]. Michigan: University of Michigan, Center for Information Technology Integration, USA, 2001: 1-11.
- [5] 张红, 周尚波. 混沌理论在密码学中的应用 [J]. 重庆大学学报: 自然科学版, 2004, 27(4): 39-43.
- Zhang Hong, Zhou Shang-bo. Application of chaos theory in cryptography [J]. Journal of Chongqing University (Natural Science Edition), 2004, 27(4): 39-43.
- [6] 王海春. 基于多混沌系统的数字密写技术 [J]. 微计算机信息, 2006, 22(33): 83-85.
- Wang Hai-chun. A steganography techniques based on three chaos system [J]. Control and Automation, 2006, 22(33): 83-85.
- [7] Xu C Y, Ping X J, Zhang T. Steganography in compressed video stream [C]// Proceedings of the First International Conference on Innovative Computing, Information and Control, 2006: 269-272.
- [8] Westfeld A, Wolf G. Steganography in a video conferencing system [C]// Proc of Information Hiding, 1998, 1525: 32-47.
- [9] Robie D L, Mersereau R M. Video error correction using data hiding techniques [C]// Multimedia Signal Processing, 2001 IEEE Forth Workshop, 2001: 59-64.
- [10] Robie D L, Wu N, Mersereau R M. The use of steganography to enhance error detection and correction in MPEG-2 video [C]// Conference Record of the Thirty-Sixth Asilomar Conference on Signals, Systems and Computers, 2002: 1204-1209.
- [11] 徐长勇, 平西建, 张涛. 视频信息伪装技术综述 [J]. 计算机应用研究, 2005, 23(12): 8-11.
- Xu Chang-yong, Ping Xi-jian, Zhang Tao. Survey of steganography in video [J]. Application Research of Computers, 2005, 23(12): 8-11.
- [12] ITU-T Rec. H.264/ISO/IEC 14496-10 AVC. Draft ITU-T recommendation and final draft international standard of joint video specification [S]. 2003.
- [13] 刘连山, 李人厚. 基于离散余弦变换直流分量的盲视频水印方案 [J]. 西安交通大学学报, 2006, 40(4): 402-405.
- Liu Lian-shan, Li Ren-hou. Blind video watermarking scheme based on direct current component in discrete cosine transformation domain [J]. Journal of Xi'an Jiaotong University, 2006, 40(4): 402-405.
- [14] Westfeld A. F5——a steganographic algorithm [C]// Proceedings of 4th International Conference on Information Hiding, LNCS 2137, Springer-Verlag, 2002: 289-302.