

基于覆盖码的多媒体传感网数据隐写算法

尤 星^{1,2} 孙 启^{1,2} 刘建坡² 童官军² 袁晓兵²

(1. 中国科学院大学计算机与通信学院, 北京, 100049; 2. 中国科学院上海微系统与信息技术研究所, 上海, 200050)

摘 要: 在多媒体传感网中进行视频信息隐藏有很多局限性。为了增强在多媒体传感网中进行隐秘通信的安全性, 本文从提高隐写效率和降低节点能耗入手, 在分析研究以往相近研究的基础上, 提出了一种新的视频信息隐藏算法。算法结合了 H. 264/AVC (Advanced video codec) 标准视频流的数据特性, 提出了调整覆盖码矩阵简化计算复杂度的新思想和避免误差漂移的隐写策略。算法运用了新的分类编码方法; 对于不同类型的数据特征, 引进并设计了针对多媒体传感网应用限制条件的覆盖编码方法。实验证明: 该算法能够降低嵌入误差, 有效抵抗统计分析; 减少了数据通信冗余, 同时计算复杂度由传统的幂次复杂度降低到线性复杂度。

关键词: 多媒体传感网; 视频隐写; 帧内预测; 覆盖码

中图分类号: TP391 **文献标志码:** A

Improved Steganography Algorithm for Multimedia Sensor Network via Coverings

You Xing^{1,2}, Sun Qi^{1,2}, Liu Jianpo², Tong Guanjun², Yuan Xiaobing²

(1. College of Computer and Communication Engineering, University of Chinese Academy of Science, Beijing, 100049, China; 2. Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Sciences, Shanghai, 200050, China)

Abstract: There are lots of constrains for video steganography in sensor networks. Based on the analysis of previous similar researches, a novel video steganography algorithm is proposed to improve steganography efficiency and reduce energy consumptions. Considering the characteristics of H. 264/AVC video stream in multimedia sensor network, this algorithm promotes a novel classification strategy having the advantages of error drift prevention and covering code adjustment with simplified calculation complexity. Furthermore, for different types of data features, we introduce and design a covering coding method satisfied the application limited conditions of multimedia sensor networks. Both data analysis and experimental results show that the proposed algorithm is robust against statistical analysis attacks and it also minimizes embedding error. With less communicating redundancy, the algorithm doubles embedding efficiency and decreases computation complexity from exponential to linear.

Key words: multimedia sensor network; video steganography; intra prediction; covering codes

引 言

随着多媒体传感器网络研究的不断深入, 其传输安全性问题越来越受到人们的重视^[1]。多媒体传

感网的特点是大数据量大信息量的采集处理,应用范围广泛,方便使用。然而由于其自身固有的特点,如信道的开放性、多硬件多节点等,使得传播各类数据的保密控制比较困难,实际应用之中存在较大的安全隐患。在一些较为敏感的应用领域,如军事战场或重要的民用公共安全设施中,传输安全问题显得更为突出。为了解决这一问题,过去在传感网应用上最常见的方法是密码学的加解密技术。这种方式虽然操作简易技术成熟,但由于加密后的信息表现出异于常规数据的不规则的特点,极易引起攻击者的注意。近年来有学者把信息隐藏技术作为一种有效的保护手段,运用在多媒体传感器网络的信息传输环境中。

信息隐藏广泛应用于数字媒体的版权保护、网络协议的身份认证、信息的隐蔽传输等方面。其最大的优点是隐蔽,但也存在一定的局限性,例如必须有庞大的隐蔽载体作掩护。在某些条件与环境下,如多媒体传感器网节点的有限通信带宽与更加复杂的信息传输格式,使得隐蔽的容量和效率受到限制。研究者通常的解决方法是从嵌入技术上寻找出路。文献[2]实现了在无线传感网环境下采用水印技术的首个系统。在此之后,研究者在多媒体传感网信息隐藏方面作了有效的探索。文献[3]指出在多媒体传感网中,不仅需要考虑常规水印系统所关注的减小图像误差和增大鲁棒性的要求,更要考虑多媒体传感网对数据传输处理的能耗限制、高差错率控制等特定要求。

尽管近年来亦不断有相应的研究^[4-10]出现,但多数的研究仍集中在水印^[6-9]或小数据量隐写上,并且以图像、音频、数据包为主要载体^[10]。视频隐写仍旧是一项难点,尤其是基于H. 264的视频流载体。而国内外用于多媒体传感网传输的流媒体越来越多地采用H. 264标准的格式,有较大的研究价值和应用前景。

本文以增强多媒体传感网的通信安全为目标,对多媒体传感网下的视频隐写应用展开深入分析。针对无线传感器网络有限的计算能力以及部分实时性要求,引入并设计覆盖码,并针对不同待选隐藏点分类选择不同的覆盖编码。在提高隐写效率同时简化计算复杂度,形成了一种新的多媒体传感网安全隐秘传输的视频隐写算法。

1 算法设计

1.1 基于H. 264的载体数据特征

应用于多媒体传感网的信息隐藏,其算法必须结合载体的特征,才能够发挥该项技术优势,增大数据隐藏的信息量,提高传感网络机密传输效率。H. 264的预测技术使得数据之间关联性很强^[11],会直接影响到信息隐藏的效率和鲁棒性。因帧内预测技术的使用,H. 264不同于传统编码技术,在该标准下的数据嵌入,如以帧内离散余弦变换(Discrete cosine transform, DCT)系数为嵌入载体,必须考虑误差漂移现象。

H. 264在IDCT(Inverse DCT)变换时,嵌入所带来的误差会扩散至原始数据的每一个像素中。设 \mathbf{X} 为原始像素残差矩阵, \mathbf{Y} 为DCT系数矩阵, $\boldsymbol{\theta}$ 为嵌入所带来的误差矩阵, $\Delta_{i,j}$ 表示原始像素矩阵中 (i,j) 点处产生的误差漂移, $Y_{i,j}$ 表示DCT系数矩阵中 (i,j) 点处的系数值, \mathbf{C}, \mathbf{E} 为IDCT变换矩阵。则误差如下

$$\mathbf{X} = \text{round}[\mathbf{C}_i^T (\mathbf{Y} \otimes \mathbf{E}_i) \mathbf{C}_i] \quad (1)$$

$$\mathbf{A} = \mathbf{X}' - \mathbf{X} = \text{IDCT}(\mathbf{Y}') - \text{IDCT}(\mathbf{Y}) = \text{IDCT}(\mathbf{Y} + \boldsymbol{\theta}) - \text{IDCT}(\mathbf{Y}) = \text{IDCT}(\mathbf{Y}) + \text{IDCT}(\boldsymbol{\theta}) - \text{IDCT}(\mathbf{Y}) = \text{IDCT}(\boldsymbol{\theta})$$

$$\Delta_{i,j} = \sum_k \text{IDCT}(\boldsymbol{\theta}_k) \quad (2)$$

如果在编码过程中用到的已编码像素存在由于信息嵌入所带来的误差,那么在当前宏块编码时,当

前宏块的预测残差就是包含误差的结果,进而误差继续通过预测向后续编码宏块传播^[12-13]。误差的累积传播如果扩散至整个 I 帧,再影响到 P 帧, B 帧的预测,整个视频编码的质量将急剧下降。这样的信息嵌入非常危险。

1.2 多媒体传感网的性能要求

以往针对预测漂移现象的解决思路主要有:通过编码后固定位置误差补偿和编码前系数成对嵌入误差消除两类方法^[12-13]。但这两类方法都是在已有信息嵌入的基础上增加额外冗余数据。额外增加的数据本质上增大了视频数据传输误差,降低了信息嵌入效率,在实际应用中存在很大问题,尤其是应用于有限资源的多媒体传感器网络。

在多媒体传感网的环境下实现信息隐藏,所研究设计的算法必须能够满足传感网有限的能源资源等条件限制,尽可能地维持和延长网络的生命周期^[1]。在增大通信效率的同时尽可能减少通信量、降低节点计算复杂度,这是节约能耗以维持多媒体传感网生存状态的主要途径。因此,从有效利用多媒体载体的数据特征和提升通信编码效率两个角度入手,是较直接和较有效的方法。

1.3 基于覆盖编码的提升编码效率方法

现代编码理论指出非线性编码的效率远大于线性编码,如著名的 Nordstrom-Robinson 码,其编码效率几乎是最好的线性码的双倍,但非线性编码的计算复杂度非常高,设计复杂,不适用于计算能力有限的多媒体传感器网络。在线性码中,一般情况下覆盖半径越大,相应的信息嵌入量越大,但于此同时造成的数据修改量也会增加,不适用于对漂移误差非常敏感的 H. 264 标准的视频流隐秘传输。

通过编码方法进行隐写嵌入,无疑可以大幅提升通信传输效率。然而编码方法的选择,对隐写的效率和复杂度影响相差很大。任何一种编码方式,显然都相较于直接替换嵌入,需要更高的节点计算处理能力。多媒体传感网的隐秘传输,既需要高效,又要避免高复杂度,构成了设计中的一对矛盾。

覆盖编码可以看成是一种空间变换方式,通过去除空间冗余,可以有效增大信息容量。但不同空间之间,转换的计算复杂度往往相差较大。利用这一特性,通过对不同类型数据的特征分析,设计有针对性的转换方式,令转换所占用的资源尽可能地降低。既切合多媒体传感网资源有限性的约束,又弥补了误差补偿所额外增加的信息占用损失,提高了秘密信息的容量,巧妙地解决了矛盾。

2 算法设计实现及数据处理

2.1 隐写分类方法

本节首先针对预测漂移现象,以提升编码效率、降低复杂度为目的,根据 H. 264 在压缩编码每一个宏块时,可能用到宏块的已编码像素分布。对视频隐写数据载体做出新的分类。

设右侧宏块预测模式为 R ,左下方宏块预测模式为 LD ,下方宏块预测模式为 D ,右下方宏块预测模式为 RD ,记各类情况组合为 $C_i (i = 1, 2, 3)$ 。标记 9 种 4×4 亮度块预测模式为 $p_i^4 (p_0^4, p_1^4, \dots, p_8^4)$,标记 4 种 16×16 亮度块预测模式为 $p_i^{16} (p_0^{16}, p_1^{16}, p_2^{16}, p_3^{16})$ 。

根据 H. 264 特殊的启发式预测编码模式,推演误差漂移传播的影响:由分布及方向看出,位于当前宏块右侧的像素块,可能会受到当前宏块最后一列像素样点的误差影响,即令 $R_1 = \{p_1^4, p_2^4, p_3^4, p_4^4, p_5^4, p_6^4, p_7^4, p_8^4, p_0^{16}, p_1^{16}, p_2^{16}, p_3^{16}\}$,取 4×4 宏块模式中的 1, 2, 4, 5, 6, 8 或 16×16 预测模式中的 1, 2, 3 任意一种时,当前宏块最后一列像素样点的误差向右侧传播。以此类推, $R_0 = \{p_0^4, p_3^4, p_7^4, p_0^{16}\}$ 时,不会产生误差传播影响。

同理, $D_1 = \{p_0^4, p_2^4, p_3^4, p_1^4, p_5^4, p_6^4, p_7^4, p_0^{16}, p_2^{16}, p_3^{16}\}$ 时,下方宏块受到当前宏块最后一行像素的误差

影响,反之, $D_0 = \{p_1^4, p_8^4, p_1^{16}\}$ 。

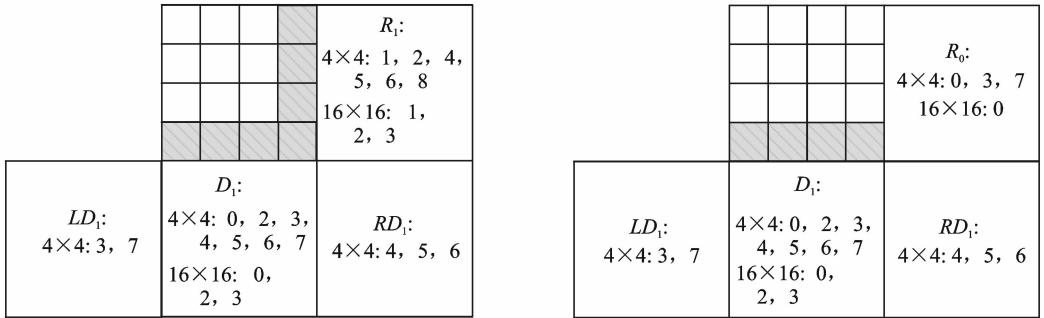
$LD_1 = \{p_3^4, p_7^4\}$ 时,左下方宏块会受到当前宏块最后一行像素的误差影响,反之, $LD_0 = \{p_0^4, p_1^4, p_2^4, p_4^4, p_5^4, p_6^4, p_8^4, p_0^{16}, p_1^{16}, p_2^{16}, p_3^{16}\}$ 。

$RD_1 = \{p_4^4, p_5^4, p_6^4\}$ 时,右下方宏块受到当前宏块最后一行像素样点的误差影响,反之, $RD_0 = \{p_0^4, p_1^4, p_2^4, p_3^4, p_7^4, p_8^4, p_0^{16}, p_1^{16}, p_2^{16}, p_3^{16}\}$ 。

为保证秘密信息在多媒体传感网中的正确传输,根据敏感像素点受到的误差影响情况,设计新的分类,为提高不同影响下的编码效率提供基础。将所有情况分为3类。

(1)当 $C_1 = R_1 \cap (D_1 \cup LD_1 \cup RD_1)$, $\Delta_{0,3} = \Delta_{1,3} = \Delta_{2,3} = \Delta_{3,3} = \Delta_{3,0} = \Delta_{3,1} = \Delta_{3,2} = 0$,此时仅一组数据可供隐写,且必须同时改动4个系数,隐写效率为1/4,即每传递1比特信息量需要修改4比特数据,效率过低,本文算法中避免在该类数据隐藏秘密信息,如图1(a)所示。

(2)当 $C_2 = R_0 \cap (D_1 \cup LD_1 \cup RD_1)$, $\Delta_{3,3} = \Delta_{3,0} = \Delta_{3,1} = \Delta_{3,2} = 0$,有 $(Y_{00}, Y_{02}), (Y_{10}, Y_{12}), (Y_{20}, Y_{22}), (Y_{30}, Y_{32})$ 4组数据可用做修改。如图1(b)所示。



(a) 符合 C_1 的数据组合
(a) Data group applied to condition C_1

(b) 符合 C_2 的数据组合
(b) Data group applied to condition C_2

图1 四周宏块预测模式对本宏块内像素的位置影响

Fig.1 Surrounding influence from different directions in current block

当 $C_3 = R_1 \cap (D_0 \cap LD_0 \cap RD_0)$, $\Delta_{0,3} = \Delta_{1,3} = \Delta_{2,3} = \Delta_{3,3} = 0$,有 $(Y_{00}, Y_{20}), (Y_{01}, Y_{21}), (Y_{02}, Y_{22}), (Y_{03}, Y_{23})$ 4组数据可用做修改。每组数据成对修改,以编码方式改进隐写效率。如图2(a)所示。

(3)当 $C_4 = R_0 \cap (D_0 \cap LD_0 \cap RD_0)$ 时,所有数据均可以任意组合方式展开数据隐写。如图2(b)所示。

2.2 基于覆盖编码的算法改进

经2.1节有效分类,对每一类数据,本文通过引入覆盖编码,有针对性地设计合适的隐写方法,优化隐写效率。

多媒体传感网在视频处理传输上的大量资源损耗,增大了隐写算法的功耗限制,决定了隐写算法必须尽可能的简化。然而隐写编码算法复杂度越大,编码效率和安全性越高。因此,隐写编码效率与算法复杂度,在多媒体传感网应用中是权衡的重要指标。本文通过调整覆盖编码的构造方法,来实现关键指标间的权衡。

令 Emb 表示嵌入映射函数: $F^n \times m \rightarrow F^n$,表示将 k 比特的秘密信息 m 嵌入载体空间 F^n ;令 Ext 表示提取过程,对应于映射函数 $Ext: F^n \rightarrow m$ 。

设 H 为 $a \times b$ 维隐写编码的传输矩阵,设任意元素 $u \in F^n, z \in F^n$ 。则嵌入过程 Emb 等同于将向量 z

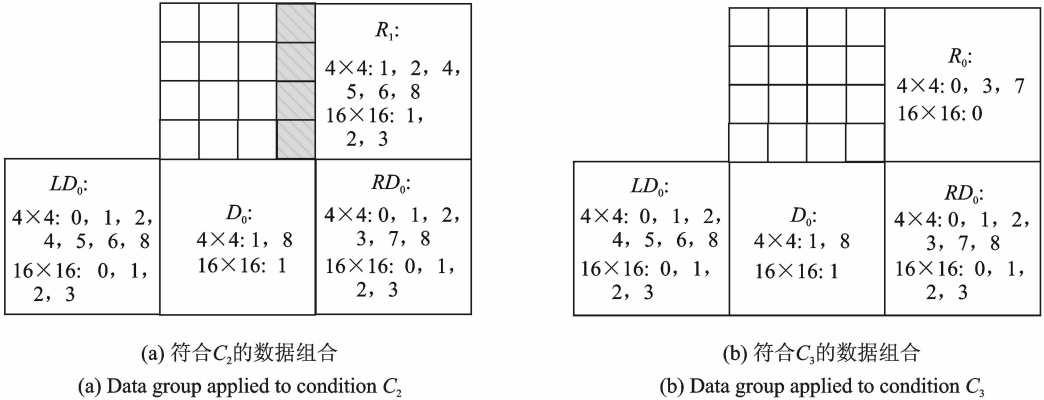


图 2 四周宏块预测模式对本宏块内像素的位置影响

Fig. 2 Surrounding influence from different directions in current block

通过传输矩阵 H 映射为向量 u , 使得向量 u 中包含秘密信息 m , s 是通过传感网传输的含密载体。即, 存在一个向量满足 $z \cdot H = u$ 。对于给定载体 v 和秘密信息 m , 有

$$z \cdot H = m - v \cdot H \tag{3}$$

$$s = v + z \tag{4}$$

$$s \cdot H = z \cdot H + v \cdot H = m \tag{5}$$

令 $w(z) = \sum_{i=1}^n z_i$ 表示向量 $z = (z_1, z_2, \dots, z_n)$ 的汉明重量, z 的实际意义在于需要对载体做多大修改, 能够得到 $s \cdot H = z \cdot H + v \cdot H = m$ 的结果。

令 ρ 表示嵌入对载体造成的最小修改量, 则

$$\rho = \min_{\{z \in B^*, z \cdot H = u\}} w(z) \tag{6}$$

其中 $z = \arg \min_{\{z \in B^*, z \cdot H = u\}} w(z)$ 。所得向量 z 必定符合最小化误差的嵌入编码矩阵。

$$\sum_{i=1}^{w(z)} \binom{N}{i} \geq F^n \tag{7}$$

令式(7)取等号, 以构造最优完备码, 保证特定误差范围内达到嵌入率上限。

在多媒体传感网应用限制条件下, 针对 2.1 节的 3 种数据分类特征, 采取两种方法: 一种是选取覆盖半径小于 3 的完备覆盖码^[14]; 另一种是特定构造形式的非完备编码^[15]。

特定构造形式的非完备编码则如下

令 $t > 0, l > 0, b - a = t + 1, a = t \times l$ 。 $\mathbf{0}_l = (0, \dots, 0) \in B^l, \mathbf{1}_l = (1, \dots, 1) \in B^l$, 可形成编码矩阵 $H_{t,l} = (\mathbf{I}_a, \mathbf{h}_0, \mathbf{h}_1, \dots, \mathbf{h}_t)$ 。其中 $\mathbf{h}_i = (h_{i,1}, \dots, h_{i,j})$, 满足

$$h_{i,j} = \begin{cases} \mathbf{0}_1 & i = j \\ \mathbf{1}_1 & i \neq j \end{cases} \tag{8}$$

在如上构造矩阵下, 在 N 比特视频流载体中隐藏 $0.75N$ 比特秘密信息, 平均只需要做出约 $0.2N$ 比特改动。针对 2.1 节的分类, 具体设置举例说明如下:

(1) 由分类 2, $b = 4$, 选取覆盖半径为 2 的 (2, 4, 3) 码, 编码矩阵具备如下形式

$$H = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix} \tag{9}$$

(2)由分类 3, $b=16$, 由于 t 越小, a 越大, 嵌入的效率越高, 则令 $t=3, l=4$, 编码矩阵如下

$$\mathbf{H} = \begin{bmatrix}
 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\
 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\
 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\
 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\
 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\
 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\
 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\
 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\
 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\
 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\
 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\
 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0
 \end{bmatrix} \tag{10}$$

2.3 嵌入提取步骤

嵌入过程可以分为如下 3 个步骤:(1)将传感器节点截取的 H. 264 视频码流经熵解码得到残差数据;将传感器节点获取的需要嵌入的秘密信息(图像、文字等)经加密形成比特流;(2)根据 2.1 节的分类方法,获取符合隐写条件的视频 DCT 系数分组;(3)根据 2.2 节的覆盖码矩阵及编码方法,可得到含密视频数据流。

提取过程可以分为 2 个步骤:(1)在传感器节点接收端,根据 2.1 节的策略选择隐藏有秘密信息的 DCT 系数载体;(2)由 $s \cdot \mathbf{H} = m$, 直接由共享的转移矩阵和载密视频数据,就可以得到秘密信息,无需传递原始载体视频,这样接收方的信息处理非常简单,可以大大节约资源消耗,非常适用于多媒体传感网的特殊应用场景。

3 实验参数和结果分析

3.1 试验条件与参数选择

采用 Matlab 对建立的模型仿真,分析在传感网环境下的秘密信息安全传输能力。依据文献[16]所用的无线传感网模型,选择 sink 节点 1 个,位置固定,100 个传感节点随机分布,其中 30 个为多媒体节点,其他节点为普通传感节点,节点通信半径为 15 m,MAC 层采用 CSMA/CA(Carrier sense multiple access/collision avoidance)协议,多媒体数据包长度为 4 kB,发送数据的周期为 8 s;普通传感节点数据包长度为 100 B,发送数据的周期为 1 s。

视频载体取自标准测试视频库,以视频序列 MOBILE, FOREMAN, BUS, CITY, CREW, FOOTBALL, HARBOUR 为测试样例,视频格式为 QCIF,以标准测试图片 Lenna 作为需要通过传感器节点之间传输的秘密信息。

3.2 视频隐写效率

表 1 数据表示秘密信息经无线多媒体传感网的传输,提取后的准确度以及各视频样例中平均每帧可传输的秘密信息比特容量。

通过计算归一化相关系数(Normalized correlation, NC)量化分析原始秘密图像与提取出的秘密图

像的相似度。NC=1 表示 2 个序列完全相同,NC 越接近 1,表示传输的准确度越高。

$$NC = \frac{\sum_i \sum_j [W(i,j) \cdot W'(i,j)]}{\sum_i \sum_j [W(i,j)]^2} \quad (11)$$

式中: $W(i,j)$ 表示传输的秘密图像的各位置点像素值; $W'(i,j)$ 则对应接收并提取得到的秘密图像。

表 1 的数据表明,不同视频载体传输的准确度略有差别,但几乎都接近 100%。本文算法与文献[13]算法选取相同限制条件,将两种算法均应用于多媒体传感网环境下,设定量化参数(Quantization parameter, QP)等于 28, $|Y_{i,j}| > 0$,得到如表 1 所示的隐写效率比较。表 1 中的算法数据指的是单帧可嵌入数据比特数。实验结果表明,隐写容量增大,性能仍然能够得到保持。

表 1 隐写效率

Table 1 Steganography efficiency

载体图像	BUS	CITY	FOREMAN	MOBILE
相关度 NC	0.998	0.999	1.000	0.998
本文算法/bit	420	390	434	362
文献[13]算法/bit	228	194	240	200

3.3 视频隐写安全性

安全性实验主要分为两个方面:视觉掩蔽性和抗干扰抗攻击能力。

图 3 中选取了上述所列 7 个测试视频样例中的前 4 个 I 帧,共 28 帧数据。对比了在采用本文算法后和采用文献[13]的算法后的隐写视频质量。以峰值信噪比(Peak signal to noise ratio, PSNR)作为衡量指标。数据表明本文算法的视频质量整体得到提升,并保持在 38 dB 以上(文献[17]证明人眼往往不能察觉峰值信噪比 38 dB 以上的影响)。

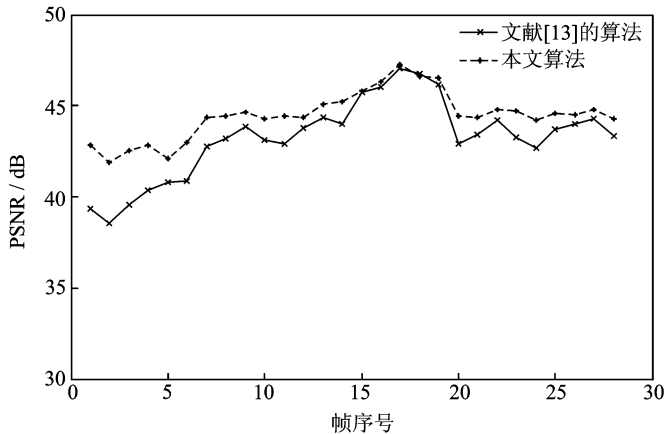


图 3 算法改进前后性能对比

Fig. 3 Contrast before and after improvements

表 2 中数据表明秘密信息在经过各类干扰攻击后的可恢复程度。实验中主要采用的干扰源是椒盐噪声、高斯滤波、均值滤波等。实验结果表明,通过加噪等模拟干扰后,提取出的秘密信息的准确率仍保持在 80%左右,在一定的误差允许范围内,可认为隐写传输抗攻击能力较强,满足秘密信息传输的安全性要求。

表 2 干扰攻击下的准确度度量

视频序列名	椒盐噪声	高斯滤波	均值滤波
MOBILE	73	83	77
FOREMAN	84	89	71
BUS	79	79	78
CITY	85	85	79

3.4 多媒体传感网的通信安全分析

本文算法中,覆盖半径为 1 的编码构造是通过奇偶校验矩阵构造,覆盖半径为 2 的编码构造则利用 PG 图求解,计算复杂度均为 $O(n)$ 。同时,文献[15]证明特定构造形式的非完备编码计算复杂度为 $O(n)$ 。相较于传统隐写编码方式,其矩阵求解的计算复杂度一般为 $O(n^2)$,本文的算法由传统的幂次复杂度降低到了线性复杂度,更符合节点的有限资源限制。

实验结果亦表明,在该算法下嵌入秘密信息传输正确率及可靠性、视频隐蔽性、抗攻击能力较高。在多媒体传感网的应用中,特别是在带宽受限的情况下,能较好地满足多媒体传感网的要求。由于计算复杂度上的改进,该算法在传感器节点上所耗费的芯片资源较少,可用于多媒体传感网上的消息验证、水印版权保护等多种场合,并能有效保护多媒体传感网的通信安全性。

4 结束语

信息隐藏是 20 世纪 90 年代刚刚兴起的一门新兴学科,随着 Internet 的迅速发展,信息隐藏技术也迅速在各方面加快渗透与运用。信息隐藏因其涉及的学科领域广泛,其原有的技术和算法都有其自身的特色和优缺点。实际应用中必须根据不同的技术条件和要求加以选择和考虑。本文抓住 H. 264 视频数据传输标准及多媒体传感网应用这 2 个特定条件,以增强多媒体传感网的通信安全为宗旨,提出一种新的隐写方案。数据分析和仿真试验表明:该方案可将数据的隐写效率提升一倍,减少了数据通信冗余度的同时还减小了传输误差,降低了节点能耗,取得了较好的应用效果。但是每种系统和算法都有各自的优缺点和局限性,要与系统整体的需要和相应程序相匹配。传感网信息的安全传输牵涉的技术很多,更可以从改进传感器效能等方面入手,也期望更多在硬件支撑和软件算法结合的研究方法的出现。

参考文献:

- [1] 罗武胜,翟永平,鲁琴. 无线多媒体传感器网络研究[J]. 电子与信息学报, 2008, 30(6): 1511-1516.
Luo Wusheng, Zhai Yongping, Lu Qin. Study on wireless multimedia sensor networks[J]. Journal of Electronics & Information Technology, 2008, 30(6): 1511-1516.
- [2] Jessica F, Miodrag P. Real-time watermarking techniques for sensor networks[C]//Electronic Imaging 2003. Santa Clara: International Society for Optics and Photonics, 2003: 391-402.
- [3] Wang Honggang, Peng Dongming, Wang Wei, et al. Energy-aware adaptive watermarking for real-time image delivery in wireless sensor networks[C]//IEEE International Conference on Communications, Beijing: IEEE, 2008: 1479-1483.
- [4] Lin Q, Wang R, Ye N, et al. Energy efficient distributed steganography for secure communication in wireless multimedia sensor networks[J]. Journal of Electronics, 2013, 30(1): 9-16.
- [5] Masood H, Usman H, Sadiq ur Rehman, et al. Secure communication in WMSN[C]//2010 International Conference on Information Networking and Automation (ICINA). [S.l.]: IEEE, 2010: 37-42.
- [6] Wang H. Communication-resource-aware adaptive watermarking for multimedia authentication in wireless multimedia sensor networks[J]. The Journal of Supercomputing, 2010(06): 1-15.
- [7] Padmavathi G, Shanmugapriya D, Kalaivani M. Digital watermarking technique in vehicle identification using wireless sensor

Networks[C]// 2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE). Chengdu, China; IACSIT, 2010; 6-10.

- [8] 陈立泽, 倪蓉蓉, 赵耀. 一种基于排序的 JPEG 码流无损水印算法[J]. 数据采集与处理, 2013, 28(2): 155-159.
Chen Lize, Ni Rongrong, Zhao Yao. Embedded lossless watermark in JPEG bitstream based on sorting[J]. *Journal of Data Acquisition and Processing*, 2013, 28(2): 155-159.
- [9] 马衍庆, 王锋, 冯峰. 基于数字水印的有线数字电视广播信息安全监测[J]. 数据采集与处理, 2012, 28(2): 246-250.
Ma Yanqing, Wang Feng, Feng Feng. Watermark-based information security monitoring for DVB-C[J]. *Journal of Data Acquisition and Processing*, 2012, 28(2): 246-250.
- [10] Harjito B, Potdar V, Singh J. Watermarking technique for wireless multimedia sensor networks; A state of the art[C]// Proceedings of the CUBE International Information Technology Conference. Pune, India; ACM, 2012; 832-840.
- [11] Kim D W, Choi Y G, Kim H S, et al. The problems in digital watermarking into intra-frames of H. 264/AVC[J]. *Image and Vision Computing*, 2010, 28(8): 1220-1228.
- [12] Huo Weijing, Zhu Yuesheng, Chen Hongyuan. A controllable error-drift elimination scheme for watermarking algorithm in H. 264/AVC stream[J]. *IEEE Signal Processing Letters*, 2011, 18(9): 535-538.
- [13] Liu Y, Li Z, Ma X, et al. A robust without intra-frame distortion drift data hiding algorithm based on H. 264/AVC[J]. *Multimedia Tools and Applications*, 2013, 72(1): 1-24.
- [14] Bierbrauer J, Fridrich J. Constructing good covering codes for applications in steganography[C]// Transactions on Data Hiding and Multimedia Security III Lecture Notes in Computer Science 4920. Berlin Heidelberg; Springer-Verlag, 2008; 1-22.
- [15] Gao Yunkai, Li Xiaolong, Yang Bin. Constructing specific matrix for efficient matrix embedding[C]// Multimedia and Expo. New York; IEEE, 2009; 1006-1009.
- [16] Wang Wei, Peng Dongming, Wang Honggang, et al. Energy efficient multirate interaction in distributed source coding and wireless sensor network[C]// Wireless Communications and Networking Conference. Kowloon; IEEE, 2007; 4091-4095.
- [17] Petitcolas F, Anderson R. Evaluation of copyright marking system[C]// Multimedia Systems. Florence, Italy; IEEE, 1999; 574-579.

作者简介: 尤星(1986-), 女, 博士研究生, 研究方向: 视频处理、信息隐藏、无线传感器网络, E-mail: livia138567@126.com; 孙启(1985-), 男, 博士研究生, 研究方向: 无线传感器网络; 刘建坡(1978-), 男, 副研究员, 研究方向: 视频信号处理、无线传感器网络; 童官军(1983-), 男, 助理研究员, 研究方向: 无线传感器网络; 袁晓兵(1969-), 男, 研究员, 博士生导师, 研究方向: 视频信号处理、无线传感器网络。

