

数字图像隐写容量的博弈分析

蒋翠玲, 庞毅林, 林家骏

(华东理工大学 信息科学与工程学院, 上海 200237)

摘 要: 提出了一种基于数字图像的新的隐写信道模型. 在该模型中, 考虑隐写分析器的作用和载体与隐秘体的相似性, 引入错误概率和检测率作为失真约束条件. 运用博弈论, 把隐写过程看成编解码方与攻击方的博弈, 给出了隐写博弈的双方在不同失真约束条件下的隐写容量, 并对容量结果进行了分析.

关键词: 信息隐藏; 隐写容量; 隐写信道; 博弈论

中图分类号: TN918.91

文献标识码: A

文章编号: 1000-7180(2010)01-0022-03

The Steganography Capacity Game Analysis Based on the Digital Images

JIANG Cui-ling, PANG Yi-lin, LIN Jia-jun

(Institute of Information and Engineering, East China University of Science and Technology, Shanghai 200237, China)

Abstract: This paper presents a new model of stego-channel based on the digital images. It takes account of the steganalysis and similarity between cover-image and stego-image, considering the probability of error and probability of detection as distortion constraints. It applies game theory to steganography. It regards the encoder-decoder and attacker as the two players in the game, analysing the steganographic capacity under different distortion constraints. At last, it discusses the results of the steganographic capacity base on the game theory.

Key words: information hiding; steganographic capacity; stego-channel; game theory

1 引言

信息隐藏技术利用人类感觉器官对数字信号的感觉冗余, 将特定信息(如版权信息、秘密信息等)嵌入到图像、语音、视频及文本文件等各种数字媒体中, 以达到标识或版权保护等目的. 隐写是信息隐藏研究的另一大分支, 用隐写载体来隐藏信息形成隐秘载体, 其作用就类似于一个带有隐藏信息的信道的传输. 因而, 可从隐写信道的角度来描述隐写的过程, 同时, 隐写信道的一个非常重要属性——隐写容量, 也是衡量一个隐写系统的重要参数指标之一. 在一个隐写系统中, 信息的隐写者和攻击者之间是对抗关系, 隐写者的目标是尽可能多地隐藏信息并通过攻击者的检查, 相反, 攻击者的目标则是尽力阻止隐秘信息的传输, 使隐秘对象的漏检率越低越好. 因此, 可借用博弈论来研究隐写系统中的隐写容量. 文献[1-3]中分析了一定率失真 D_1 和 D_2 的约束条件

下, 信道分布服从高斯分布和信道不带参数情况下水印的博弈问题. 文中主要从不同分类的隐写信道的角度出发, 采用错误概率和检测率作为失真约束度量的方法, 分析不同博弈情况下的隐写容量.

2 隐写博弈的问题描述

从博弈论的角度, 隐写的过程可看成两个局中人的博弈, 即一方为信息的隐藏者(编码者)和解码者, 另一方则为攻击者. 在隐写中, 假定攻击是无记忆的, 可以把隐写容量看成是信息的隐藏者与攻击者之间的互信息的博弈. 信息的隐藏者为了获得最大收益, 他会尽可能优化载体信道, 即最大最小化(maxmin)支付矩阵, 而攻击者为了获得最大收益, 会尽可能优化无记忆的攻击信道, 即最小化(minimize)支付矩阵. 在此博弈中, 一个局中人的付出是另一个局中的所得, 每一次的双方得失之和为零, 因此, 双方的行为符合二人有限零和博弈. 文献[1]中

讨论了信息隐藏中的博弈理论,考虑了在不同失真约束下的马鞍点的具体解决,对于无参的攻击模型该如何设计最佳的信息隐藏算法^[4].

Moulin^[3,5]的隐写信道模型如图1所示,在一个隐写系统中,假定待嵌入的信息为 M , 长度为 N . 载体信号 S^N 用序列表示为: $S^N = (S_1, \dots, S_N)$, 隐写中的加密密钥或者编 - 解码方共享的边信息(side information)表示为 $K^N = (K_1, \dots, K_N)$. 因此,隐写后的信息可表示为 $X^N = (X_1, \dots, X_N) = f_N(S^N, M, K^N)$. 在此过程中,会受到外在的攻击 A^N , 试图从 X^N 中消除或修改 M . 假定攻击后输出的序列为 $Y^N = (Y_1, \dots, Y_N)$. 解码方收到 Y^N 并采用编码方相反的处理来估计出嵌入的信息 $\hat{M}$.

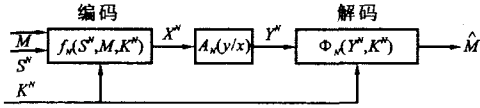


图1 Moulin的隐写系统图

博弈双方的支付矩阵表示为 $\Psi(f_N, A_N, \Phi_N)$, 其中,隐写中的编 - 解码算法函数可描述为 $DH = (f_N, \Phi_N)$, 攻击信道为 A_N , A_N 的可行性集取决于在一定的失真约束下 f_N 的选择. Φ_N 的可行性集独立于 f_N 和 A_N 的选择. 对于攻击方,假定在抗最恶劣攻击下的编 - 解码算法函数为 $DH^f = (f_N, \Phi_N)^f$, 则有

$$\Psi^*(DH^*, A_N^*) = \max_{A_N} \Psi(DH^f, A_N) \quad (1)$$

而事实上,没有其他的攻击比此种状况更糟,所以有

$$\forall A_N, \Psi(DH^f, A_N) \leq \Psi^*(DH^*, A_N^*) \quad (2)$$

对于编 - 解码方,在最小的攻击策略 A_N^* 时如何获得最优的编 - 解码算法 DH^* , 即如何解决:

$$(DH^*, A_N^*) = \arg \min_{DH} \max_{A_N} \Psi(DH, A_N) \quad (3)$$

则在 A_N^* 的情况下,

$$\forall DH, \Psi(DH^*, A_N^*) \leq \Psi(DH, A_N^*) \quad (4)$$

于是该博弈的纳什均衡为

$$\Psi(DH, A_N^*) \leq \Psi(DH^*, A_N^*) \leq \Psi(DH^*, A_N) \quad (5)$$

3 基于博弈的隐写容量

基于 Moulin 的隐写信道模型^[3,5], 文中提出了一种新的隐写信道的框架模型,如图2所示. 在此模型中,我们定义了两大信道类型. 第一类型信道(编码 - 噪声信道 W^N) 描述由于隐写过程中内在的编

——解码函数产生的失真. 第二类型信道(攻击信道 A^N) 描述一些恶意的攻击,如对隐写信号的裁剪或加性噪声等. 为描述编码 —— 噪声信道与攻击信道之间的作用,引入了编码 —— 攻击信道 Q^N 的概念.

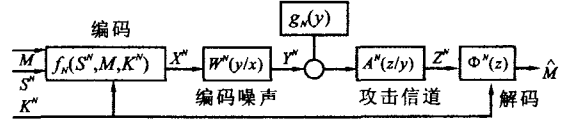


图2 一种新的的隐写信道模型

图2中,一个无记忆的检测器用 $g = \{g_n\}_{n=1}^{\infty}$ 表示, $y = (y_1, y_2, \dots, y_n)$, 则

$$g_n(y) = \begin{cases} 1, & \text{if } \exists i \in \{1, 2, \dots, n\}, g(y_i) = 1 \text{ 有隐写} \\ 0, & \text{if } g(y_i) = 0, \forall i \in \{1, 2, \dots, n\}, \text{没有隐写} \end{cases} \quad (6)$$

定义1 一个编码 - 噪声信道表示为 W^N , 其中, $W^N: Y^N \times X^N \rightarrow [0, 1]$, 对于 $x \in X^N$, 有

$$W^N(y | x) := \Pr\{Y^N = y | X^N = x\} \quad (7)$$

定义2 攻击信道: 假定攻击函数 $A_N: Y^N \times Z^N$, 则攻击信道可表示为

$$A_N(z | y) := \Pr\{Z^N = z | Y^N = y\}, \quad A := \{A_1, A_2, A_3, \dots\}. \quad (8)$$

定义3 一个专用的编码 —— 攻击信道 Q^N 是一个函数: $X^N \rightarrow Z^N$ 传输的概率序列, 表示为

$$Q = \{Q^1, Q^2, Q^3, \dots\}. \text{ 其中} \quad Q^N(z | x) = \sum_{y \in Y^N} A^N(z | y) W^N(y | x) \quad (9)$$

定义4 对每一个输入的 x_i , 如果信道失真独立并且同分布的, 则该信道称为无记忆信道, 表示为^[2,4]

$$W^N(y | x) = \prod_{i=1}^N W(y_i | x_i) \quad (10)$$

在此隐写的信道模型中, 考虑失真约束度量为错误概率 ϵ_n (Probability of Error, 编 - 解码方的错误概率) 和为检测率 δ_n (Probability of Detection). 错误概率表示为

$$\epsilon_n = 1/M_N \sum_{i=1}^{M_N} Q^N(D_i^c | u_i) \quad (11)$$

式中, D_i 表示解码序列, 信息隐写后的编码表示为 $f_N(i) = u_i, i \in \{1, \dots, M_n\}$, 即编码序列表示为 $c = \{u_1, \dots, u_{M^N}\}$, $Q^N = A^N$. W^N , 假定待嵌入的信息是一个服从统一分布的信息集合, 其集的势表示为 M_N .

隐写分析时的检测率表示为

$$\delta_n = 1/M_N \sum_{i=1}^{M_N} W^N(I_{GN} | u_i) \quad (12)$$

式中, $I_{GN} = g_N^{-1}(\{1\}) = \{y \in y^N : g_N(y) = 1\}$

定理 1 假定 $N \geq 1$, 解码方已知攻击信道 A_N 和 f_N , 同时攻击者已知编码方 f_N , 在失真约束 ϵ_n 和 δ_n 的条件下, 信息的嵌入速率为 R , 则隐写容量为

$$\text{Cap} = \max_{W(y, u|s, k) \in W} \min_{A(z|y) \in A} \Psi(W, A) \quad (13)$$

式中, 把博弈中的互信息作为支付矩阵, 表示为 $\Psi(W, A)$, 有

$$\begin{aligned} \Psi(W, A) &= I(U; Z | K) - I(U; S | K) \\ &= I(U; Z, K) - I(U; S, K) \\ &= H(U | S, K) - H(U | Z, K) \end{aligned} \quad (14)$$

式中, U 是一个辅助的随机变量, 定义在一个集 μ 中, 且 $|\mu| \leq |W| + 1$.

对于 $\forall A, \Psi(f_N, A^N, \Phi_N) \leq \Psi^*$. 如果能够找到理想的编 - 解码算法 (f_N^*, Φ_N^*) , 最小的攻击策略 A^* , 使之满足式(3), 则 (f_N^*, A^*, Φ_N^*) 就是式(5)中的纳什均衡中的马鞍点.

推论 1: 考虑一种特殊的情况, 如果 $K = S$, 则编 - 解码方共享载体的全部信息, 则隐写容量为

$$\text{Cap} = \max_{p(y|s)} \min_{A(z|y)} I(Y; Z | S) \quad (15)$$

证明: 如果 $K = S$, 则式(14)中的支付矩阵 $\Psi(W, A) = I(U; Z | S) = I(U, S; Z | S) \leq I(Y; Z | S)$, 而 $(U, S) \rightarrow X \rightarrow Y \rightarrow Z$ 是一个马尔可夫链, 当 X 是 (S, U) 的函数时取等号, 式(14)由 S 与 Y 的联合分布概率密度函数 $p(y | s)$ 来决定 $W(x, u | s)$, 进一步确定 $\Psi(W, A)$ 的值, 从而式(15)得证.

推论 2: 隐写博弈的容量的上界为考虑一种特殊的情况, 如果是被动攻击, 即 $Z = Y$, 并且 $K = S$, 则

$$\text{Cap} = \max_{p(y|s)} H(Y | S) \quad (16)$$

如果 $Z = Y$, 由推论 1 可得 $\text{Cap} = \max_{p(y|s)} H(Y | S)$. 如果是 $K = S$ 由 $\Psi(W, A) = I(U; Y) - I(U, S) = H(U | S) - H(U | Y)$, 假定 $U = Y$, 则 Cap 的最大值是 $H(U | S)$, 这也是式(15)中的容量的上界, 从而式(16)得证.

推论 3: 隐写博弈的容量的下界为

$$\text{Cap} \geq \max_{p(y|s, k)} [H(Y | S, K) - \max_{A(z|y)} H(Y | Z, K)] \quad (17)$$

证明: 由式(14), 要使其值最小, 则当约束编码 - 噪声信道 W^N 的最大值为 $U = Y$ 时, 则由式(13)

可得

$$\text{Cap} \geq \max_{W(y|s, k) \in W} \min_{A(z|y) \in A} [I(Y; Z | K) - I(Y; S | K)]$$

结合式(14), 则得到式(17).

4 博弈隐写的容量结果分析

(1) 如果解码者知道攻击者所使用的攻击信道, 或者从接收到的信息中能够可靠地估计出攻击信道, 则式(13)容量的界的取值是可实现的. 基于一个典型的已有的攻击信道, 该如何设计一个通用的解码器, 仍是隐写面临的一个需要解决的问题.

(2) 定理 1 可看做在满足某种失真约束条件下的容量博弈的问题. 最优化的攻击是解决率失真问题, 也反应了信息论中数据压缩的重要性. 最优化的信息隐藏理论就是解决受约束条件的容量问题.

(3) 在许多传统的信息隐藏算法中, 把 U 看做独立于 S 的变量. 这种做法一般不是最优的, 式(14)反应的是数据的可靠传输速率是在 $I(U; Z | K)$ 取最大值的上限.

5 结束语

文中针对从隐写信道不同分类的角度出发, 提出了一种新的隐写信道模型, 考虑了在一个隐写系统中隐写分析器(检测器)的作用和载体与隐秘体之间的关系. 运用博弈理论, 把隐写系统的编-解码方、攻击方作为博弈中的两个局中人, 把博弈双方的互信息作为支付矩阵, 提出了把错误概率和检测率作为隐写系统失真约束的度量方法, 分析了在不同情况下博弈双方的支付矩阵与隐写容量的关系. 由于文中的研究现在还只限于理论阶段, 如何运用博弈论的知识, 针对某一种通用的隐写信道模型如何来设计最优的信息隐藏算法和攻击算法是以后进一步研究的重点.

参考文献:

- [1] Alvaro A Cairdenas, George V Moustakides, John S Baras. Towards optimal design of data hiding algorithms against nonparametric adversary models[C]//Information Sciences and Systems, CISS '07. 41st Annual Conference. Baltimore, 2007: 911-916.
- [2] Harmsen J, Pearlman W. Capacity of steganographic channels[C]//Proc. of the 7th workshop on Multimedia and Security. New York, 2005(1/2):11-24.

(下转第 28 页)

表 1 带隙基准电路对比表

Specifications	文献[3]	文献[5]	proposed
Technology	0.18 μm CMOS	0.18 μm CMOS	0.18 μm CMOS
Supply voltage range/V	1.5~2.5	1.6~3	1.5~3.3
Temperature range/ $^{\circ}\text{C}$	-40~80	30~150	-40~125
Reference voltage/V	0.713	1.45	0.8016
Temperature coefficient/ (ppm/ $^{\circ}\text{C}$)	8@1.8V	23@1.8V	2.7@1.8V
Line Regulation	76 $\mu\text{V/V}$	2.1mV/V	1.2mV/V

路的工作电压范围为 1.5V~3.3V, 且在此范围内线性调整率为 1.2mV/V.

参考文献:

- [1] Leung K N, Mok P K T, Leung C Y. A 2V 3uA 3ppm/ $^{\circ}\text{C}$ curvature - compensated BiCMOS bandgap reference [J]. IEEE Journal of Solid - State Circuits, 1994, 38(3): 561 - 564.
- [2] Wang Xichuan, Si Cuiying, Xu Xing. Curvature compensated CMOS bandgap reference with 1.8V operation[C]//

High Density Microsystem Design and Packaging and Component Failure Analysis, HDP'06. Shanghai, 2006: 20 - 23.

- [3] Hou Ming Chen, Chih Liang Huang, Robert C Chang. A new temperature compensation CMOS bandgap reference circuit for portable applications[C]// Circuits and Systems, ISCAS 2006. Proceedings. 2006 IEEE International Symposium on. Island of KOS, 2006: 4.
- [4] Banba H, Shiga H, Umezawa A, et al. A CMOS bandgap reference circuit with sub - 1 V operation[J]. IEEE Journal of Solid - state Circuits, 1999, 34(5): 670 - 674.
- [5] Xing Xinpeng, Li Dongmei, Wang Zhihua. A novel CMOS current mode bandgap reference[J]. Journal of Semiconductors, 2008, 29(7): 1249 - 1253.
- [6] 盛庆华, 张亚君, 王红义. 一种线性补偿的带隙基准电路 [J]. 微电子学与计算机, 2007, 24(1): 169 - 172.

作者简介:

许小丽 女, (1985 -), 硕士研究生. 研究方向为模拟集成电路分析与设计.

冯全源 男, (1963 -), 博士, 教授, 博士生导师, IEEE 高级会员. 研究方向为集成电路设计、半导体材料及器件、微波及毫米波技术、移动天线与智能天线系统、自适应信息处理、电磁兼容与环境电磁学、微波器件及材料等.

(上接第 24 页)

- [3] Pierre Moulin, Kivanc Mihca M. The parallel - gaussian watermarking game[J]. IEEE Transactions on Information Theory, 2004, 50(20): 1 - 6.
- [4] Harmsen J. Secure capacity of steganographic systems[D]. New York, Polytechnic Institute Troy, 2005.
- [5] Pierre Moulin, Joseph A O'Sullivan. Information - theoretic analysis of information hiding[J]. IEEE Transactions on Information Theory, 2003, 49(2): 19 - 23.
- [6] Jiang Cuiling, Lin Jiajun, Pang Yilin. Capacity analysis of steganography based on the digital images under the constraints of security[C]// International Conference on Au-

dio, Language and Image Processing. Shanghai: East China University of Sci. & Technol., 2008(7): 909 - 912.

- [7] 蒋翠玲, 林家骏, 庞毅林. 基于数字图像隐写容量的分析 [J]. 微电子学与计算机, 2008, 25(4): 72 - 76.
- [8] 于祺, 陈克非. 基于图像的广义隐写分析[J]. 微电子学与计算机, 2008, 25(6): 212 - 215.

作者简介:

蒋翠玲 女, (1976 -), 讲师, 博士研究生. 研究方向为图像处理、信息隐藏.

林家骏 男, 博士生导师, 教授.

庞毅林 男, 讲师.