大容量自适应隐写对抗的博弈研究

刘 静,汤光明
(解放军信息工程大学,河南郑州 450001)

摘 要: 攻击方拥有自适应规范边信息条件下,如何提高大容量自适应隐写的安全性成为亟待解决的问题.本文对大容量自适应隐写方和攻击方进行博弈建模,分析了博弈均衡存在的条件,通过理论证明给出均衡局势下隐写对抗双方的混合策略和期望支付,最后利用仿真实验验证了理论分析的正确性.研究表明,攻击方的策略与嵌入的信息量无关,期望支付随着嵌入信息量的增加而增加;隐写方选择在载体中某位置进行较多嵌入的概率随着该位置的复杂度增加而增加且不为零.该结论对设计安全的大容量自适应隐写具有一定的指导意义.

关键词: 隐写;博弈论;大容量;均衡局势
中图分类号: TN918.91 **文献标识码:** A **文章编号:** 0372-2112 (2014)10-1963-07
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2014.10.015

Game Research on Large-Payload and Adaptive Steganographic Counterwork

LIU Jing, TANG Guang-ming
(*PLA Information Engineering University, Zhengzhou, Henan* 450001, *China*)

Abstract: Given that the attacker has the side information of adaptivity criterion, it is an urgent problem for the steganographer to improve the security of large-payload and adaptive steganography. This paper proposed a game-theoretic model for the two sides. Through theoretical derivation, we provided the necessary conditions for game equilibrium, along with the mixed strategies and expected payoffs of the two sides in equilibrium. Results of numerical simulation validated the theoretical analysis. This research reveals that the attacker's strategy is independent of the number of hidden bits, and the expected payoff increases with the number of hidden bits. The probability that one position is selected by steganographer to embed more bits is always greater than zero and increases with the complexity of that position. These conclusions bring some guidance for devising secure adaptive steganography with large payload.

Key words: steganography; game theory; large-payload; equilibrium

1 引言

自适应隐写是利用人眼对图像复杂纹理区域不敏感[1]这一特性,在图像内容相对复杂的区域嵌入较多信息,在图像内容相对简单的区域嵌入较少信息[2~6]或不嵌入任何信息[7~11].这类方法都是通过选取一个自适应规范,如像素差,局部方差等,来实现收发双方的同步.随着隐写检测技术[12,13]的发展,相比于随机均匀嵌入,自适应隐写被广泛地认为可以更好的抵抗隐写检测.然而,用来测试的检测算法并非专门针对自适应隐写而设计,因此这一认知未遵从 Kerckhoffs 准则:攻击方拥有隐写方的自适应规范边信息甚至可能估计出相应的自适应规范阈值.Böhme 等[14]指出若检测方分析得到文献[7]中的自适应规范,文献[7]中给出的自适应隐写方案的安全性将低于随机均匀嵌入,Tan 等[15]分析得到文献[8]中自适应规范阈值,对文献[8]中的自适应隐写实施了有效检测.这些研究都对自适应隐写的安全性提出了挑战.如何在满足 Kerchhoffs 准则下,设计安全的自适应隐写成为一个重要的课题.

博弈论是解决隐写方和攻击方对抗关系的有效手段.Schöttle 等[16]利用博弈理论研究了载体只包含两个复杂度不同且相互独立的元素,同时攻击方了解何元素更适合嵌入时,隐写方选择对何元素进行嵌入可提高抗检测能力.他们指出总选择在相对复杂的元素进行嵌入

收稿日期:2013-05-30;修回日期:2013-09-28;责任编辑:孙瑶
基金项目:国家自然科学基金(No.61101112);中国博士后基金(No.2011M500775);河南省科技攻关计划(No.122102210047)

反而会降低隐写的安全性.随后,Johnson 等[17]对文献[16]中的工作进行扩展,研究了载体包含 n 个复杂度不同且相互独立的元素时,隐写方和攻击方达到均衡时的混合策略.假设攻击方知道载体每个元素的概率分布,但这一假设会过高估计攻击方的能力,为了使攻击方的能力更接近实际,又假设一次对抗中攻击方只能利用一个元素的概率分布进行局部判断.研究结果表明:对载体的每个元素都以一定的概率进行嵌入的方案,优于仅选择相对复杂元素进行嵌入的方案.上述研究工作都是围绕"在什么位置进行嵌入"展开,一个位置最多携带一比特信息.若要实现更高的隐写容量,隐写方和攻击方需要选择何种策略以达到均衡,目前并未见有公开文献予以讨论.本文在 Schöttle 和 Johnson 的研究工作基础上,沿用 Johnson 等[17]关于载体元素相互独立以及攻击方能力的假设,利用博弈理论围绕"在什么位置进行较多嵌入"展开研究,给出了博弈均衡的条件和均衡局势下隐写方和攻击方的混合策略以及期望支付.

2 问题描述

令 Alice 为隐写方,Eve 为攻击方.Alice 在共享密钥控制下利用嵌入算法将秘密消息嵌入到原始载体中,并将隐秘载体通过公开信道进行传送.Eve 监视着公开信道,对信道上传输的载体进行检测,并判断是原始载体还是隐秘载体.博弈在 Alice 和 Eve 之间展开.令 $X=(X_0,\cdots,X_{n-1})$ 为载体,是由 n 个 m 比特数据组成的序列,每个数据的取值空间为 $\{0,\cdots,2^m-1\}$,且 X 中的各个元素相互独立.

为了反映隐写的自适应性,利用文献[16]中提出的载体生成模型表示载体元素的复杂度:

$$P(X_i=x_i)=f_{t_i}^0(x_i)$$
$$=(2^m-x_i)t_i+\left(1-\left(\sum_{j=1}^{2^m}j\right)t_i\right)/2^m \quad (1)$$

其中,$x_i\in\{0,\cdots 2^m-1\}$,$i\in\{0,\cdots,n-1\}$,$t_i\in\left[0,\left(\sum_{j=1}^{2^m-1}j\right)^{-1}\right)$.$f_{t_i}^0(x_i)$表示原始载体第 i 个元素 X_i 取值为 x_i 的概率.可以看出,在该模型中 t_i 决定了第 i 个载体元素的复杂度.当 $t_i=0$ 时,$f_{t_i}^0(x_i)$为均匀分布,此时该元素最为复杂,因此也最适合进行较多嵌入.随着 t_i 的增加,第 i 个载体元素的复杂度随之减少.

由于二比特替换是大容量隐写中最简单也最常见的修改方式,在国内外研究中受到广泛关注[18,19],因此,为了简化分析,本文将大容量隐写的修改方式建模为二比特替换,对于可进行较多嵌入的载体元素采用最低两位替换隐写,其他则采用最低位替换隐写.文献[2~4]等提出的大容量自适应隐写方法也均可归为此类修改方式.不失一般性,将 $x\in\{0,\cdots,2^m-1\}$的取值空间定义为{0,1,2,3},即取 $m=2$,此时,$t_i\in[0,1/6)$.

3 博弈模型

3.1 Alice 的策略

假设 Alice 需要在 $X=(X_0,\cdots,X_{n-1})$ 的一个实值序列 $x=(x_0,\cdots,x_{n-1})$ 上翻转 k 个比特以隐藏一段信息.因此,Alice 的策略集是集合 $x'=(x_{0,0},x_{0,1},\cdots,x_{n-1,0},x_{n-1,1})$ 的 k 维子集的集合,其中 $x_{i,0}$和 $x_{i,1}$分别表示 x_i 的最低位比特和次低位比特.她的混合策略是这些 k 维子集上的一个概率分布.令 G 为某个 k 维子集,$A(G)$ 为 Alice 选择在 G 上进行翻转的概率,则:

$$\begin{cases}A(G)\geq 0, G\subset x'\\ \sum_{G\subset x'}A(G)=1\end{cases} \quad (2)$$

令 $A(i,j)$ 为 Alice 选择在 $x_{i,j}$, $i\in\{0,\cdots,n-1\}$, $j\in\{0,1\}$处进行翻转的概率,则:

$$\begin{cases}A(i,j)=\sum_{x_{i,j}\in G}A(G)\geq 0\\ \sum_{i=0}^{n-1}\sum_{j=0}^{1}A(i,j)=k\end{cases} \quad (3)$$

根据式(2)和(3)可将 Alice 的混合策略由 $A(G)$ 转化为 $A(i,j)$.

3.2 Eve 的策略

Eve 需要判断她所观察的实值序列 $x=(x_0,\cdots,x_{n-1})$是原始载体还是隐秘载体.她的最优判断规则是利用 $X=(X_0,\cdots,X_{n-1})$ 的联合概率分布进行似然比检验.然而在实际隐写对抗中,Alice 和 Eve 都不可能知道载体 $X=(X_0,\cdots,X_{n-1})$ 的联合概率分布.本文沿用文献[17]对攻击方能力的假设,即 Eve 知道 $X=(X_0,\cdots,X_{n-1})$ 的边缘分布 $P(X_i\leq x_i)$, $i\in\{0,\cdots,n-1\}$,但一次对抗中 Eve 只能利用一个位置的边缘分布做最优局部判断.因此,Eve 的混合策略是在 n 个位置上的一个概率分布 $E=(E(0),\cdots,E(n))$,其中 $E(i)$,$i\in\{0,\cdots,n-1\}$表示 Eve 选择观察第 i 个位置的概率.

3.3 Eve 的判断规则

令 $f_{t_i}^1(x_i)$ 为在载体第 i 个元素 X_i 中嵌入消息后 X_i 取值为 x_i 的概率,有:

$$\begin{aligned}f_{t_i}^0(x_i)&=P(x_i\mid Cover);\\ f_{t_i}^1(x_i)&=P(x_i\mid Stego)\end{aligned} \quad (4)$$

引理 1 根据载体生成模型和本文的嵌入方式,隐秘载体的概率质量函数 $f_{t_i}^1(x_i)$为:

$f_{t_i}^1(x_i)=$

$$\begin{cases} f^0_{t_i}(x_i) - (A(i,0) + 3A(i,0)A(i,1) + 2A(i,1))t_i, x_i = 0 \\ f^0_{t_i}(x_i) + (A(i,0) - A(i,0)A(i,1) - 2A(i,1))t_i, x_i = 1 \\ f^0_{t_i}(x_i) - (A(i,0) - A(i,0)A(i,1) - 2A(i,1))t_i, x_i = 2 \\ f^0_{t_i}(x_i) + (A(i,0) + 3A(i,0)A(i,1) + 2A(i,1))t_i, x_i = 3 \end{cases} \tag{5}$$

证明　当 $x_i = 0$ 时:

$$\begin{aligned} f^1_{t_i}(x) &= A(i,0)f^0_{t_i}(x_i+1) + A(i,0)A(i,1)f^0_{t_i}(x_i+3) \\ &\quad + A(i,1)f^0_{t_i}(x_i+2) \\ &= A(i,0)\left[(2^k - (x_i+1))t_i + \left(1 - \left(\sum_{j=1}^{2^m} j\right)t_i\right)/2^m\right] \\ &\quad + A(i,1)\left[(2^k - (x_i+2))t_i + \left(1 - \left(\sum_{j=1}^{2^m} j\right)t_i\right)/2^m\right] \\ &\quad + A(i,0)A(i,1)\left[(2^k - (x_i+3))t_i + \left(1 - \left(\sum_{j=1}^{2^m} j\right)t_i\right)/2^m\right] \\ &= f^0_{t_i}(x_i) - (A(i,0) + 3A(i,0)A(i,1) + 2A(i,1))t_i \end{aligned} \tag{6}$$

同理可得当 $x_i = 1, x_i = 2$ 和 $x_i = 3$ 时,$f^1_{t_i}(x_i)$的表达式,如式(5)所示.　证毕

引理 2　对于某一载体数据 x_i,Eve 的最优判断规则是:

$$DR(x_i) = \begin{cases} Cover, & x_i = 0 \\ Stego, & x_i = 3 \\ Cover/Stego, & 其他 \end{cases} \tag{7}$$

证明　本文借助最大后验概率(MAP)估计[16,20]实施判决.判决结果由下式表示:

$$\hat{\theta} = \arg\max_{\theta} P(\theta \mid x_i) = \arg\max_{\theta} P(x_i \mid \theta) \cdot P(\theta) \tag{8}$$

其中,$\theta \in \{Cover, Stego\}$,由于 Eve 截获到原始载体和隐秘载体的概率都为 1/2,因此有:$P(\theta) = P(Cover) = P(Stego) = 1/2$.根据式(4),有:

$$\hat{\theta} = \arg\max_{\theta} P(x_i \mid \theta) = \arg\max_{\theta} \{f^0_{t_i}(x_i), f^1_{t_i}(x_i)\} \tag{9}$$

根据式(5):

当 $x_i = 0$ 时:$f^0_{t_i}(x_i) > f^1_{t_i}(x_i)$,由式(9):$\hat{\theta} = Cover$.

当 $x_i = 3$ 时,$f^0_{t_i}(x_i) < f^1_{t_i}(x_i)$,由式(9):$\hat{\theta} = Stego$.

当 $x_i = 1$ 和 $x = 2$ 时,根据式(5)无法判断 x 是否携带信息,因此 Eve 的最优判断是分别以 1/2 的概率判断为原始载体和隐秘载体.　证毕

3.4　博弈结果

由于 Alice 的目标是增加 Eve 的判断错误率以提高隐写的安全性,而 Eve 的目标是减少自己的判断错误率.因此,Alice 和 Eve 的对抗实质上是二人有限零和博弈,本文将其支付矩阵定义如表 1 所示.

定理 1　令 $E(i)$为 Eve 的混合策略,$A(i,j)$为 Alice 的混合策略,$i \in \{0,\cdots,n-1\}$,$j \in \{0,1\}$,则(Eve, Alice)的期望支付为:

$$\left(\sum_{i=0}^{n-1} t_i E(i)(2A(i,1) + A(i,0)),\right.$$

$$\left. -\sum_{i=0}^{n-1} t_i E(i)(2A(i,1) + A(i,0))\right) \tag{10}$$

表 1　Eve 和 Alice 的支付矩阵(Eve, Alice)

		实际情况	
		原始载体	隐秘载体
Eve 的判断	原始载体	(1, -1)	(-1, 1)
	隐秘载体	(-1, 1)	(1, -1)

证明　首先假设 Eve 以 1 的概率观察 x_i.在实际中,Eve 截获到的是原始载体还是隐秘载体的概率均为 1/2.Eve 仅观察 x_i 时,她赢得的概率为:

$$\begin{aligned} P(\text{在 } x_i \text{ 上 Eve 赢}) &= \frac{1}{4} + \frac{1}{2}\begin{pmatrix} f^0_{t_i}(0) + f^0_{t_i}(0)A(i,0)A(i,1) \\ + f^0_{t_i}(1)A(i,1)(1 - A(i,0)) \\ + f^0_{t_i}(2)A(i,0)(1 - A(i,1)) \\ + f^0_{t_i}(3)(1 - A(i,0))(1 - A(i,1)) \end{pmatrix} \\ &= \frac{1}{4} + \frac{1}{2}\begin{pmatrix} f^0_{t_i}(0) + f^0_{t_i}(3) + \left(f^0_{t_i}(1) - f^0_{t_i}(3)\right)A(i,1) \\ + \left(f^0_{t_i}(2) - f^0_{t_i}(3)\right)A(i,0) \\ + \left(f^0_{t_i}(0) - f^0_{t_i}(1) - f^0_{t_i}(2) + f^0_{t_i}(3)\right)A(i,0)A(i,1) \end{pmatrix} \end{aligned} \tag{11}$$

而:$f^0_{t_i}(0) - f^0_{t_i}(1) = t_i$,$f^0_{t_i}(2) - f^0_{t_i}(3) = t_i$,$f^0_{t_i}(1) - f^0_{t_i}(3) = 2t_i$,$f^0_{t_i}(0) + f^0_{t_i}(3) = 1/2$.

可得:

$$P(\text{在 } x_i \text{ 上 Eve 赢}) = \frac{1}{2} + \frac{t_i}{2}(2A(i,1) + A(i,0)) \tag{12}$$

因此,Eve 在 $x = (x_0, \cdots, x_{n-1})$ 上的赢得概率为:

$$\begin{aligned} &\sum_{i=0}^{n-1} E(i)\left(\frac{1}{2} + \frac{t_i}{2}(2A(i,1) + A(i,0))\right) \\ &= \frac{1}{2} + \frac{1}{2}\sum_{i=0}^{n-1} t_i E(i)(2A(i,1) + A(i,0)) \end{aligned} \tag{13}$$

Eve 的期望支付为:

$$\begin{aligned} &P(\text{Eve 赢}) \cdot 1 + P(\text{Eve 输}) \cdot (-1) \\ &= \frac{1}{2} + \frac{1}{2}\sum_{i=0}^{n-1} t_i E(i)(2A(i,1) + A(i,0)) \\ &\quad - \frac{1}{2} + \frac{1}{2}\sum_{i=0}^{n-1} t_i (2A(i,1) + A(i,0)) \\ &= \sum_{i=0}^{n-1} t_i E(i)(2A(i,1) + A(i,0)) \end{aligned} \tag{14}$$

因此可得(Eve, Alice)的期望支付如式(10)所示.　证毕

4　博弈均衡

4.1　博弈均衡的必要条件

推论 1　Alice 与 Eve 的博弈存在均衡的必要条件之一是:

$$A(i,0) - A(i,0)A(i,1) - 2A(i,1) = 0 \tag{15}$$

证明　由引理 1、引理 2 以及定理 1 的证明过程

知:若 $A(i,0)-A(i,0)A(i,1)-2A(i,1)>0$ 则当 Eve 观察到 $x_i=1$ 时,则将其判断为隐秘载体,观察到 $x_i=2$ 时,将其判断为原始载体,此时可计算得到 P(在 x_i 上 Eve 赢)的概率与 $A(i,0)$有关而与 $A(i,1)$ 无关.Alice 可通过增加 $A(i,1)$,减少 $A(i,0)$,使 $A(i,0)-A(i,0)A(i,1)-2A(i,1)<0$ 使 Eve 判断错误.因此不存在均衡.同理可得若 $A(i,0)-A(i,0)A(i,1)-2A(i,1)<0$ 也不存在均衡.所以只有当 $A(i,0)-A(i,0)A(i,1)-2A(i,1)=0$ 时,使引理 2 保持成立,才存在均衡. 证毕

为了便于模型求解,本文引入 Eve 的单个优势和 Eve 的总体优势两个定义.

定义 1 (Eve 的单个优势) Eve 在 X_i 上的优势为 $t_i(A(i,1)+A(i,0))$.

定义 2 (Eve 的总体优势) Eve 的总体优势是在 $X_0,\cdots,X_{n-1}$上的单个优势的加权和,即 $\sum_{i=0}^{n-1} t_i E(i)(A(i,1)+A(i,0))$.

由于对整个博弈过程来说,Eve 的目标是尽可能地增加她的期望支付,而 Alice 的目标是尽可能地减少 Eve 期望支付,由推论 1,Alice 和 Eve 的博弈存在均衡的必要条件为:

$$A(i,0)=2A(i,1)/(1-A(i,1)) \tag{16}$$

可知 $A(i,0)$随着 $A(i,1)$增加而增加,因此 Eve 的总体优势随着 $A(i,1)$的增加而增加,当:

$$\sum_{i=0}^{n-1} t_i E(i)(A(i,1)+A(i,0)) > \sum_{i=0}^{n-1} t_i E(i)(A'(i,1)+A'(i,0)) \tag{17}$$

有:

$$\sum_{i=0}^{n-1} t_i E(i)(A(i,1)) > \sum_{i=0}^{n-1} t_i E(i)A'(i,1) \tag{18}$$

因此 Eve 的期望支付:

$$\sum_{i=0}^{n-1} t_i E(i)(2A(i,1)+A(i,0)) > \sum_{i=0}^{n-1} t_i E(i)(2A'(i,1)+A'(i,0)) \tag{19}$$

由上可将对期望支付的分析转化为对 Eve 优势的分析,即 Eve 的目标是增大她的优势,而 Alice 的目标是减少 Eve 的优势.

引理 3 Alice 和 Eve 的博弈存在均衡的必要条件之二是 Eve 在 $X_0,\cdots,X_{n-1}$上的单个优势均相等,即:

$$t_i(A(i,1)+A(i,0))=t_j(A(j,1)+A(j,0)) \quad i,j\in\{0,\cdots,n-1\},i\neq j \tag{20}$$

证明 若 Eve 在 $X_0,\cdots,X_{n-1}$上的单个优势不相等,那么总有 Eve 在某个 $X_i,i\in\{0,\cdots,n-1\}$上的单个优势小于 Eve 在 $X_j,j\in\{0,\cdots,n-1\},j\neq i$ 上的单个优势,即 $t_i(A(i,1)+A(i,0))<t_j(A(j,1)+A(j,0))$.此时,Eve 可通过令 $E(j)=E(j)+E(i),E(i)=0$ 使得其总体优势相比于原来增加:

$$E(i)(t_j(A(j,1)+A(j,0))-t_i(A(i,1)+A(i,0)))>0 \tag{21}$$

因此这种情况下不存在均衡. 证毕

引理 4 Alice 和 Eve 的博弈存在均衡的必要条件之三是:

$$t_i E(i)=t_j E(j),\quad i,j\in\{0,\cdots,n-1\},i\neq j \tag{22}$$

证明 若存在 i,j,当 $i\neq j$ 时有,$t_i E(i)<t_j E(j)$,则 Alice 可通过令 $A(j,1)+A(j,0)=0,A(i,1)+A(i,0)=A(j,1)+A(j,0)+A(i,1)+A(i,0)$使得 Eve 的总体优势增加:

$$\begin{aligned}&t_i E(i)(A(j,1)+A(j,0)+A(i,1)+A(i,0))\\&-t_i E(i)(A(i,1)+A(i,0))\\&-t_j E(j)(A(j,1)+A(j,0))\\&=(A(j,1)+A(j,0))(t_i E(i)-t_j E(j))<0\end{aligned} \tag{23}$$

因此,这种情况不存在均衡. 证毕

4.2 Alice 的唯一混合策略

根据均衡存在的必要条件,引理 5 给出了均衡局势下,Alice 存在的唯一混合策略.

引理 5 在均衡局势下,Alice 的唯一混合策略为:

$$A(i,0)=\frac{1}{2}\left(k/t_i\sum_{j=0}^{n-1}\frac{1}{t_j}-3+\sqrt{\left(k/t_i\sum_{j=0}^{n-1}\frac{1}{t_j}-3\right)^2-8k/t_i\sum_{j=0}^{n-1}\frac{1}{t_j}}\right) \tag{24}$$

$$A(i,1)=\frac{1}{2}\left(k/t_i\sum_{j=0}^{n-1}\frac{1}{t_j}+3-\sqrt{\left(k/t_i\sum_{j=0}^{n-1}\frac{1}{t_j}-3\right)^2-8k/t_i\sum_{j=0}^{n-1}\frac{1}{t_j}}\right) \tag{25}$$

证明 根据引理 3,均衡存在必要条件:

$$t_i(A(i,1)+A(i,0))=t_j(A(j,1)+A(j,0)) \tag{26}$$

令 $t_i(A(i,1)+A(i,0))=C,i\in\{0,\cdots,n-1\},C$ 为一常数,有:

$$A(i,1)+A(i,0)=\frac{C}{t_i} \tag{27}$$

而根据式(3),有:

$$\sum_{i=0}^{n-1}(A(i,1)+A(i,0))=k \tag{28}$$

因此:

$$\sum_{i=0}^{n-1}(A(i,1)+A(i,0))=k=\sum_{i=0}^{n-1}\frac{C}{t_i} \tag{29}$$

可得:

$$C=k/\sum_{i=0}^{n-1}\frac{1}{t_i} \tag{30}$$

因此有如下方程:

$$\begin{cases} A(i,1) + A(i,0) = k/t_i \sum_{j=0}^{n-1} \frac{1}{t_j} \\ A(i,1) = A(i,0)/(A(i,0)+2) \end{cases} \tag{31}$$

求解 $A(i,0)$和 $A(i,1)$,可得式(24)和(25). 证毕

4.3 Eve 的唯一混合策略

下面的引理给出了均衡局势下,Eve 存在的唯一混合策略.

引理 6 在均衡局势下,Eve 的唯一混合策略为:

$$E(i) = 1/t_i \sum_{j=0}^{n-1} \frac{1}{t_j} \tag{32}$$

证明 根据引理 4,有:

$$t_i E(i) = t_j E(j),\quad i,j \in \{0,\cdots,n-1\}, i \neq j \tag{33}$$

令 $t_i E(i) = C, i \in \{0,\cdots,n-1\}$, C 为一常数,则:$E(i) = C/t_i$,由于 $\sum_{j=0}^{n-1} E(j) = 1$,因此:

$$C = 1/\sum_{j=0}^{n-1} \frac{1}{t_j} \tag{34}$$

从而可得 $E(i)$如式(32)所示. 证毕

4.4 均衡局势下的博弈结果及分析

定理 2 对于要翻转 k 比特的大容量自适应隐写,当 Alice 选择翻转第 i 个位置的最低位的概率$A(i,0)$和次低位的概率 $A(i,1)$分别如式(24)和(25)所示,Eve 观察第 i 个位置的概率 $E(i)$如式(32)所示时,该博弈存在唯一混合策略纳什均衡,Eve 和 Alice 期望支付(Eve, Alice)为:

$$\left(\sum_{i=0}^{n-1} \left(\frac{3k/t_i \sum_{j=0}^{n-1} \frac{1}{t_j} - 3 - \left(\left(k/t_i \sum_{j=0}^{n-1} \frac{1}{t_j} + 1 \right)^2 + 8 \right)^{\frac{1}{2}}}{2\sum_{j=0}^{n-1} \frac{1}{t_j}} \right) \right.$$

$$\left. - \sum_{i=0}^{n-1} \left(\frac{3k/t_i \sum_{j=0}^{n-1} \frac{1}{t_j} - 3 - \left(\left(k/t_i \sum_{j=0}^{n-1} \frac{1}{t_j} + 1 \right)^2 + 8 \right)^{\frac{1}{2}}}{2\sum_{j=0}^{n-1} \frac{1}{t_j}} \right) \right) \tag{35}$$

证明 根据引理 5 和引理 6,Eve 的期望支付:

$$\begin{aligned} &\sum_{i=0}^{n-1} t_i E(i)(2A(i,1) + A(i,0)) \\ &= \sum_{i=0}^{n-1} t_i E(i) \left(k/t_i \sum_{j=0}^{n-1} \frac{1}{t_j} + 3 - \left(\left(k/t_i \sum_{j=0}^{n-1} \frac{1}{t_j} + 1 \right)^2 + 8 \right)^{\frac{1}{2}} \right) \\ &+ \sum_{i=0}^{n-1} t_i E(i) \frac{1}{2} \left(k/t_i \sum_{j=0}^{n-1} \frac{1}{t_j} - 3 + \left(\left(k/t_i \sum_{j=0}^{n-1} \frac{1}{t_j} + 1 \right)^2 + 8 \right)^{\frac{1}{2}} \right) \\ &= \sum_{i=0}^{n-1} \left(\frac{3k/t_i \sum_{j=0}^{n-1} \frac{1}{t_j} - 3 - \left(\left(k/t_i \sum_{j=0}^{n-1} \frac{1}{t_j} + 1 \right)^2 + 8 \right)^{\frac{1}{2}}}{2\sum_{j=0}^{n-1} \frac{1}{t_j}} \right) \end{aligned} \tag{36}$$

证毕

推论 2 在均衡局势中,Eve 的混合策略与 k 无关,Eve 的期望支付随着 k 的增加而增加.

证明 由引理 6 可知 Eve 的混合策略与 k 无关.对 Eve 的期望支付关于 k 求导,可得:

$$\sum_{i=0}^{n-1} \left(\frac{3k/t_i \sum_{j=0}^{n-1} \frac{1}{t_j} + 3 - \left(\left(k/t_i \sum_{j=0}^{n-1} \frac{1}{t_j} + 1 \right)^2 + 8 \right)^{\frac{1}{2}}}{2\sum_{j=0}^{n-1} \frac{1}{t_j}} \right)' \Bigg|_k > 0 \tag{37}$$

因此,在均衡局势中,Eve 的期望支付随着需要翻转的比特数 k 的增加而增加. 证毕

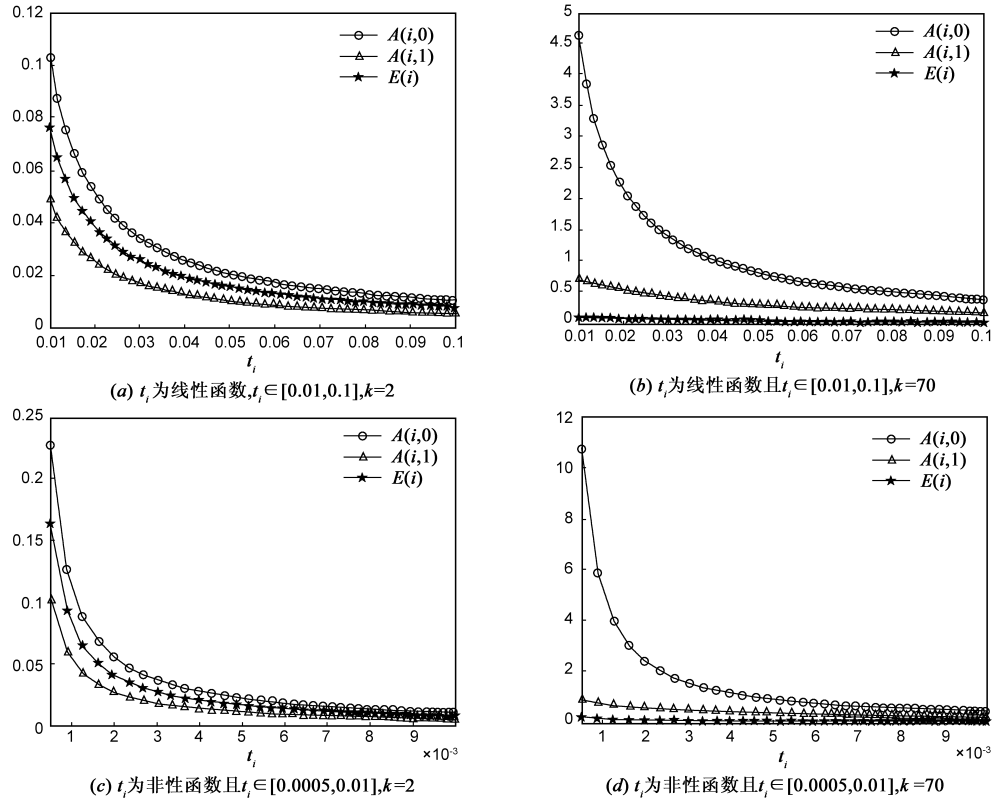
5 仿真实验

图 1 给出了 $n = 50$ 时,四种不同情形均衡局势下 Alice 和 Eve 的混合策略 $A(i,0)$, $A(i,1)$和 $E(i)$.其中图 1(a)和图 1(b)中 t_i 为线性函数且$t_i \in [0.01, 0.1]$, k 的取值分别为 2 和 70.图 1(c)和图 1(d)中 t_i 为非性函数,且 $t_i \in [0.0005, 0.01]$, k 的取值也分别为 2 和 70.

从图 1 可以看出,$A(i,0)$, $A(i,1)$都随着 t_i 的增加而减小,这符合在复杂区域进行嵌入的安全性要高于在简单区域进行嵌入的安全性这一经验结论,也说明了自适应隐写相较于随机均匀嵌入的优势. $A(i,0) > A(i,1)$表明在最低位进行嵌入的安全性高于在次低位进行嵌入的安全性.同时,对所有的 i,都有 $A(i,1) > 0$,说明隐写方应该利用所有的载体元素进行较多嵌入,而不是仅仅只选择在较复杂的元素进行较多嵌入.

6 结论

本文利用二人零和博弈研究了在载体中隐藏大容量信息的隐写对抗问题.隐写方选择在何处嵌入较多信息,攻击方选择何处进行观察,从而可利用该处分布进行最优局部判断.通过博弈分析,给出了均衡存在的条件,证明了该博弈存在唯一混合策略纳什均衡并给出了均衡局势下隐写方和攻击方的期望支付.研究表明,均衡局势下,载体中的任何元素都应该以一定的概率被隐写方选择进行较多嵌入,攻击方的策略与嵌入的信息量无关,但其检测成功率随着嵌入信息量的增多而增加.在均衡局势下,大容量自适应隐写博弈与一比特自适应隐写博弈[16,17]的攻击方策略是一致的,均只与载体元素的复杂度有关;大容量隐写模式中隐写方选择载体某一元素进行较多嵌入的概率也与一比特模式中隐写方选择载体某一元素进行一比特嵌入的概率类似,均不为零且随着载体元素的复杂度增加而增加,但大容量隐写模式还要求选择在载体元素次低位进行嵌入的概率要低于在最低位进行嵌入的概率.



(*a*) t_i为线性函数,t_i∈[0.01,0.1],k=2

(*b*) t_i为线性函数且t_i∈[0.01,0.1],k=70

(*c*) t_i为非性函数且t_i∈[0.0005,0.01],k=2

(*d*) t_i为非性函数且t_i∈[0.0005,0.01],k=70

图1 n=50时四种不同情形均衡局势下Alice和Eve的混合策略

本文仅分析了二比特替换为修改方式的隐写博弈,但对于要嵌入更多比特的修改方式,如多比特替换,或其他类型的修改方式,如,$\pm l(l=1,2,3,\cdots)$等,仍可利用本文提出的博弈方法进行分析.在这些修改方式下,隐秘载体的概率质量函数分析过程较为复杂,得到的隐秘载体概率质量函数也会不同于二比特替换,因此 Eve 的判决规则也会不同.利用本文的博弈方法,研究在这些修改方式下隐写方和攻击方采取何种策略以达到均衡将是我们未来工作的重点.需要说明的是,本文进行博弈分析时,沿用了文献[17]中的假设,这些假设都只是对现实的抽象和近似,与实际仍存在一定的距离.在后续工作中,我们将使假设条件更接近现实,以独立同分布的元素组为对象进行分析,进一步弥合理论与实践的鸿沟.

参考文献

[1] 郭云彪,尤新刚,张春田,周琳娜.面向信息隐藏的图像复杂度研究[J].电子学报,2006,34(6):1048 – 1052.
Guo Yun-biao, You Xin-gang, Zhang Chun-tian, Zhou Lin-na. Study of image bit-plane complexity in the information hiding [J]. Acta Electronica Sinica, 2006, 34(6): 1048 – 1052. (in Chinese)

[2] H C Wu, N I Wu, C S Tsai, M S Hwang. Image steganographic scheme based on pixel-value differencing and LSB replacement methods[J]. IEE Proceedings-Vision, Image and Signal Processing, 2005, 152(5): 611 – 615.

[3] B Nguyen, S Yoon, H Lee. Multi bit plane image steganography [A]. Proceedings of International Workshop on Digital Watermarking[C]. Berlin: Springer, 2006. 61 – 70.

[4] C H Yang, C Y Weng, S J Wang, H M Sun. Adaptive data hiding in edge areas of images with spatial LSB domain systems [J]. IEEE Transactions on Information Forensics and Security, 2008, 3(3): 488 – 497.

[5] 戴跃伟,刘光杰,叶曙光.基于 Hilbert 填充曲线的自适应隐写[J].电子学报,2008,36(12A):35 – 38.
Dai Yue-wei, Liu Guang-jie, Ye Shu-guang. Adaptive steganography based on Hilbert filling curve[J]. Acta Electronica Sinica, 2008, 36(12A): 35 – 38. (in Chinese)

[6] W Hong. Adaptive image data hiding in edges using patched reference table and pair-wise embedding technique[J]. Information Sciences, 2013, 221(1): 473 – 489.

[7] E Franz. Steganography preserving statistics properties[A]. Proceedings of 5th International Workshop on Information Hiding[C]. Noordwijkerhout: Springer, 2002. 278 – 294.

[8] W Luo, F Huang, J Huang. Edge adaptive image steganography based on LSB matching revisited[J]. IEEE Transaction on Information Forensics and Security, 2010, 5(2): 201 – 214.

[9] W Luo, F Huang, J Huang. A more secure steganography based on adaptive pixel-value differencing scheme [J]. Multimed Tools Application, 2011, 52(2 – 3): 407 – 430.

[10] T Pevny, T Filler, Bas P. Using high-dimensional image models to perform highly undetectable steganography [A]. Proceedings of 12th International Conference on Information Hiding [C]. Calgary: Springer, 2010. 161 – 177.

[11] T Filler, J Fridrich. Design of adaptive steganographic schemes for digital images [A]. Proceedings of SPIE, Electronic Imaging, Security and Forensics of Multimedia XIII [C]. San Francisco: SPIE, 2011. 1 – 14.

[12] 张良.一种基于幅度预测的隐写分析方法[J].电子学报,2010,38(11):2704 – 2707.
Zhang liang. A steganalysis scheme using magnitude prediction [J]. Acta Electronica Sinica, 2010, 38(11): 2704 – 2707. (in Chinese)

[13] 毛家发,钮心忻,杨义先,时书剑.基于 JPEG 净图定量描述的隐写分析方法[J].电子学报,2011,39(8):1907 – 1912.
Mao Jia-fa, Niu Xin-xin, Yang Yi-xian, Shi Shu-jian. Steganalysis method based on JPEG cover image quantitative describing [J]. Acta Electronica Sinica, 2011, 39(8): 1907 – 1912. (in Chinese)

[14] R Böhme, A Westfeld. Exploiting preserved statistics for steganalysis [A]. Proceedings of 6th International Workshop on Information Hiding [C]. Toronto: Springer, 2004. 82 – 96.

[15] S Tan, B Li. Targeted steganalysis of edge adaptive image steganography based on LSB matching revisited using B-spline fitting [J]. IEEE Signal Processing Letters, 2012, 19(6): 336 – 339.

[16] P Schöttle, R Böhme. A game-theoretic approach to content-adaptive steganography [A]. Proceedings of 14th International Conference on Information Hiding [C]. Berkeley: Springer, 2012. 125 – 141.

[17] B Johnson, P Schöttle, R Böhme. Where to hide the bits? [A]. Proceedings of Third International Conference on Decision and Game Theory for Security [C]. Budapest: Springer, 2012. 1 – 17.

[18] A D Ker. Steganalysis of embedding in two least-significant bits [J]. IEEE Transactions on Information Forensics and Security, 2007, 2(1): 46 – 14.

[19] 罗向阳,刘粉林,杨春芳,廉士国.一类自适应隐写的更改比率估计[J].中国科学:信息科学,2011,41(3):297 – 310.
Luo Xiang-yang, Liu Fen-Lin, Yang Chun-fang, Lian Shi-guo. Modification ratio estimation for a category of adaptive steganography [J]. Science China: Information Sciences, 2011, 41(3): 297 – 310. (in Chinese)

[20] Fridrich J. Steganography in Digital Media: Principles, Algorithms, and Applications (1st Ed) [M]. New York: Cambridge University Press, 2009. 10 – 12.

作者简介

刘　静　女.1985 年 11 月出生,安徽宣城人.2007 年和 2010 年分别在解放军信息工程大学电子技术学院获学士、硕士学位.现为解放军信息工程大学博士研究生,主要研究方向为数字隐写.
E-mail: kimi_liujing@163.com

汤光明　女.1963 年 1 月出生,湖南常德人.解放军信息工程大学教授、博士生导师.主要从事信息安全、信息隐藏等方面的研究工作.
E-mail: tgm1983@sina.com