第 34 卷 第 9 期 计 算 机 工 程 2008 年 5 月
Vol.34 No.9 Computer Engineering May 2008
·安全技术· 文章编号：1000—3428(2008)09—0172—02 文献标识码：A 中图分类号：TP309.2

# 基于图像信息隐藏的抗提取性评价

韩杰思[1]，沈建京[1]，袁 媛[2]
(1. 解放军信息工程大学理学院，郑州 450001；2. 双流国税局，成都 610021)

**摘 要：**对隐藏密钥的概念进行定义，定义其为包括算法选择密钥$K_1$、图像载体选择密钥$K_2$和嵌入位置、顺序选择密钥$K_3$在内的三元组。通过分析$K_1$，$K_2$的具体意义以及度量$K_3$的计算复杂度，对基于图像信息隐藏系统的抗提取性进行了评价，对安全性领域的研究具有一定的指导意义。

**关键词：**信息隐藏；隐藏密钥；抗提取性

# Property of Protection from Distilling Evaluation Based on Image Information-hiding

HAN Jie-si[1], SHEN Jian-jing[1], YUAN Yuan[2]
(1. Institute of Science, PLA Information Engineering University, Zhengzhou 450001; 2. Shuangliu National Taxation, Chengdu 610021)

**【Abstract】** In the context, the concept of hiding key is defined that it is a function with three elements including $K_1$, the secret key to choose the arithmetic, $K_2$, the secret key to choose the image, and $K_3$, the secret key to choose the positions and sequence of embedding. Based on the analysis of the meanings of $K_1$, $K_2$, and the measurement of the counting complexity of $K_3$, the property of protection from distilling of the information hiding system based on the image is evaluated, and it has instructional significance in the research of the field of security.

**【Key words】** information-hiding; hiding key; property of protection from distilling

信息隐藏技术的发展已经成为信息安全领域的研究热点，很多专家学者致力于信息隐藏算法和模型的研究。近年来，许多优秀的算法和模型不断问世。在很多算法和模型中，经常会出现一个所谓“隐藏密钥”的概念，然而对这个概念的理解却没有达成一致。

抗提取性是指在攻击者成功检测出隐藏信息存在的情况下，试图从隐秘载体中提取出秘密信息的难度。针对一个具体的信息隐藏系统来说，如果攻击者成功地检测出了信息隐藏的存在，进而再成功地提取出了隐藏的秘密信息则会造成更加严重的后果；但如果攻击者仅仅检测出信息隐藏的存在而无法从隐秘载体中提取出秘密信息，那么他也只是让这个信息隐藏系统不再有效，而无法知道通信双方的通信内容。所以说抗提取性是评价一个信息隐藏系统好坏的重要因素，也是信息隐藏系统在被攻破情况下不得不考虑的重要特性。

针对这 2 个重要的问题，本文对隐藏密钥的概念进行了全新的定义，对其进行了详细的解释；并从隐藏密钥计算复杂度的角度出发对图像信息隐藏的抗提取性进行了评价，希望对解决这 2 个问题有所帮助。

## 1 信息隐藏系统的隐藏密钥

1883 年，Kerckhoffs给出了密码系统的第一设计准则[1]，他在该准则中建议：保密系统中所使用的加密体制和算法都应当是公开的，系统的的安全性必须也只能依赖于密钥的选取。借鉴Kerckhoffs准则，可得：

在攻击者成功地检测出隐秘载体中隐藏着秘密信息，并且已经知道所使用的隐藏算法，还具有很强的计算能力，但并不知道隐藏密钥的情况下是无法从隐秘载体中提取出秘密信息的。

整个基于图像的信息隐藏系统的信息嵌入过程可用图 1 来表示。众所周知，对于一个图像信息隐藏系统来说，进行秘密信息的嵌入首先要选取合适的隐藏算法，接着要选择合适的图像载体；最后才在选中的图像载体中选择合适的嵌入位置和嵌入顺序，利用选好的隐藏算法进行秘密信息的嵌入。

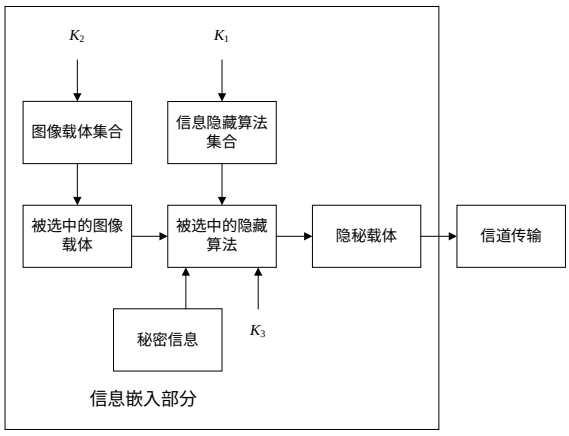


**图 1 信息的嵌入过程**

于是，对隐藏密钥进行了定义：用来控制整个信息隐藏过程的密钥集合。它主要包括信息隐藏算法的选择密钥，图像载体的选择密钥，秘密信息嵌入位置以及嵌入顺序的选择密钥。

**基金项目：**国家部委科研预研基金资助项目
**作者简介：**韩杰思(1981－)，男，博士研究生，主研方向：人工智能，信息隐藏；沈建京，教授、博士生导师；袁 媛，学士
**收稿日期：**2007-04-21 **E-mail：**jacksonhanrabbit@163.com

可用一个三元组来表征隐藏密钥：

$K=(K_1,K_2,K_3)$

其中，$K$指的就是隐藏密钥；而$K_1$，$K_2$，$K_3$分别指代的是算法选择密钥，图像载体选择密钥和嵌入位置、顺序选择密钥。

从图 1 可以看出整个信息搭载部分完全是通过隐藏密钥来进行控制的。而信息的提取部分是嵌入部分的一个逆过程，原理基本是一样的。它需要从隐秘载体中提取出秘密信息，故需要用到$K_1$和$K_3$，而对于非盲提取隐藏算法，在提取的时候还需要用到$K_2$。

考虑信息隐藏的抗提取性必须假设攻击者掌握了所有的隐藏算法，而且已经明确判断出了秘密信息的存在。如果在这样的前提条件下，攻击用尽各种办法仍然无法从隐秘载体中成功地提取出秘密信息，那么就说明隐藏系统具有良好的抗提取性。

## 2 信息隐藏抗提取性评价

根据Kerckhoffs准则，所有的隐藏算法都是公开的。但是现有的隐藏算法多种多样，即使攻击者已经掌握了所有的隐藏算法，但他拿到一幅待测图像并不知道里面是否隐藏有秘密信息，也不知道发送方是用何种算法将秘密信息嵌入的。所以通过密钥$K_1$可以增大攻击者提取的难度，让他在不知道$K_1$有的情况下不得不用相当数量的破解算法进行尝试，来判断发送方用何种方式嵌入秘密信息，及秘密信息的隐藏区域。

发送方可以通过控制$K_2$使原始载体图像不被攻击者获取，这样攻击者面临的就将是唯隐秘载体图像攻击。如果攻击者获取了原始载体图像，将会在很大程度上降低提取秘密信息的难度，这是由于 $H[M\mid(C,C')]<H(M)$ (这里的$M$是指秘密信息，$C$是指原始载体图像，$C'$是指隐秘载体图像)。因此控制$K_2$，也是为了提高攻击者提取秘密信息的难度。

$K_3$作为系统的嵌入位置、顺序选择密钥，是真正用来保证系统抗提取性的。攻击者要进行秘密信息的提取面临的最大问题也就是如何获取$K_3$。通过度量$K_3$的计算复杂度可以刻画系统的抗提取性。

假设$K_1$选定了空域LSB隐藏算法[2]，$K_2$选定的载体图像的大小为 $M\times N$，而要隐藏的秘密信息的长度为$L$。现在就要通过$K_3$在载体图像的LSB上选取$L$个位置将秘密信息隐藏进去。在这里，$L\le(M\times N)$。

对于一幅图像来说，它的最低位平面所携带的图像信号的能量极少，已经看不出任何图像的轮廓了，近似于一幅杂乱无章的二值图像。而秘密信息在嵌入到载体前通常经过加密处理，呈现出来的也是随机的乱数[3]。所以，无论采用何种方式嵌入，即无论通过$K_3$如何选取嵌入位置和嵌入顺序，想要提取秘密信息的难度是一样的。此时攻击者只知道秘密信息的长度$L$和秘密信息所在区域，即图像最低位平面的 $M\times N$ bit，要想提取出秘密信息的难度就等同于对长为$L$的密文信息进行唯密文攻击，其计算复杂度为 $C_{M\times N}^{L/2}$ (对加密后的信息来说，0,1 的个数一般各为$L$/2)。

如果秘密信息在嵌入到载体前没有进行任何预处理，那么攻击者可以考虑对秘密信息各位之间的相关性进行分析，这样可以在一定程度上降低计算复杂度。

因为到目前为止还没有任何的信息隐藏提取算法问世，所以说考虑隐藏密钥的计算复杂度时没有考虑秘密信息内各位之间的相关性，只考虑完全穷尽的情况。

对于一个数字图像信息隐藏系统来说，嵌入的秘密信息长度 $L$ 是一个非常大的数，而图像的大小比 $L$ 更大，所以，提取秘密信息的计算复杂度 $C_{M\times N}^{L/2}$ 是一个极为庞大的数目。

对于其他的隐藏算法，无论空间域还是变换域也都一样，攻击者通过对隐秘图像进行分析检测只能确定秘密信息的嵌入区域和秘密信息的长度，而无论它的检测算法如何好，它所能确定的秘密信息嵌入区域的大小 $S$ 也大于等于 $L$。即使$S$=$L$，它想提取出秘密信息计算复杂度也是 $C_L^{L/2}$。

在设计信息隐藏系统的时候，只要保证这个数目次数的计算超过现有的硬件的计算能力，使要完成这个计算需要花费很长的时间，就可以说现阶段要想从载体图像中提取出秘密信息是不可能的。在嵌入秘密信息的时候，为了保证系统的抗提取性，通常采用随机选取位置进行嵌入。这样相当于秘密信息在载体中进行了置乱，让攻击者没有任何相关性可循，不得不进行穷尽攻击。

## 3 结束语

信息隐藏技术已经受到越来越多人的关注，它的发展已经进入到了一个新的时期。作为一门新兴学科，它的理论还没有建立起来，这将是今后很长一段时期内研究的发展方向。而作为理论研究的重点，安全性的研究更是相当欠缺。

本文的研究目的就是为了对安全性理论的研究做出一些贡献，而这些研究还很不成熟，还有很多地方需要考虑，这也是笔者今后的研究重点。

## 参考文献


[1] Kerkhoffs A. La Cryptographie Militaire[J]. Journal des Sciences Militaires, 1883, 9(2): 5-38.

[2] 汪小帆, 戴跃伟, 茅耀斌. 信息隐藏技术方法与应用[M]. 北京: 机械工业出版社, 2001.

[3] Goldreich O. 密码学基础[M]. 北京: 人民邮电出版社, 2005.


（上接第 171 页）


[2] Yang Chouchen, Chang Tingyi, Hwang Min-Shiang. A (*t*,*n*) Multi-secret Sharing Scheme[J]. Applied Mathematics and Computation, 2004, 151(2): 483-490.

[3] Pang Liaojun, Wang Yumin. A New (*t*,*n*) Multi-secret Sharing Scheme Based on Shamir's Secret Sharing[J]. Applied Mathematics and Computation, 2005, 167(2): 840-848.

[4] Li Huixian, Cheng Chuntian, Pang Liaojun. A New (*t*,*n*) Threshold Multi-secret Sharing Scheme[C]//Proceedings of the 25th Annual IACR Crypto'05. Berlin, Germany: Springer-Verlag, 2005: 421-426.

[5] 黄东平, 王华勇, 黄连生, 等. 动态门限秘密共享方案[J]. 清华大学学报: 自然科学版, 2006, 46(1): 102-105.

[6] Stallings W. 密码编码学与网络安全: 原理与实践[M]. 2 版. 杨明, 胥光辉, 齐望东, 等, 译. 北京: 电子工业出版社, 2001.