

数字隐写模型及形式化描述

宋海涛, 汤光明, 孙怡峰, 王洋

(信息工程大学, 河南 郑州 450001)

摘 要: 为了使数字隐写模型研究与隐写技术研究同步发展, 从通用到具体, 依次提出3个数字隐写模型, 并对各模型进行形式化描述, 总结梳理隐写算法的本质原理, 以指导隐写技术的进一步发展。首先, 针对已有模型无法描述新兴隐写算法的问题, 提出一个通用数字隐写模型, 以描述当前所有隐写算法; 其次, 鉴于载体修改式的隐写算法在隐写术研究中的重要地位, 提出基于载体修改的加性噪声隐写模型; 然后, 针对当前主流的图像自适应隐写算法, 提出具体的最小化失真的数字图像自适应隐写模型。选取4个典型的隐写算法实例, 采用所提隐写模型进行对应描述, 以验证所提模型的有效性。

关键词: 隐写术; 隐写模型; 通用隐写模型; 载体修改式隐写模型; 自适应隐写模型

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2020036

Digital steganography model and its formal description

SONG Haitao, TANG Guangming, SUN Yifeng, WANG Yang

Information Engineering University, Zhengzhou 450001, China

Abstract: In order to make the research of digital steganography model develop synchronously with steganography research, three digital steganography models from general to specific are proposed, and each model was formalized. Through study on digital model, the essential principles of steganography algorithm were summarized to guide the further development of steganography. Firstly, aiming at the problem that the existing model cannot describe the emerging steganography algorithms, a general digital steganography model was proposed to describe nearly all steganography algorithms. Secondly, in view of the important position of the cover modification steganography algorithm in the research of steganography, a cover-modification digital steganography model was proposed. Then, for the current mainstream image adaptive steganography algorithm, a digital image adaptive steganography model with minimal distortion was proposed. Four typical steganography algorithm were selected as examples which were described by the proposed steganography model to validate the effectiveness of the proposed model.

Key words: steganography, steganography model, general steganography model, cover-modification steganography model, adaptive steganography model

收稿日期: 2019-03-25; 修回日期: 2019-08-08

通信作者: 宋海涛, kernelsong@yeah.net

基金项目: 国家自然科学基金 (61601517)

Foundation Item: The National Natural Science Foundation of China (61601517)

论文引用格式: 宋海涛, 汤光明, 孙怡峰, 等. 数字隐写模型及形式化描述[J]. 网络与信息安全学报, 2020, 6(3): 59-65.

SONG H T, TANG G M, SUN Y F, et al. Digital steganography model and its formal description[J]. Chinese Journal of Network and Information Security, 2020, 6(3): 59-65.

1 引言

近 20 年来, 隐写术取得了快速发展, 其以隐藏秘密信息“存在”的方式保证信息安全, 为用户隐私保护、敏感信息安全传输提供了有效途径。一直以来, 专家学者着力于视觉不可感知和统计抗检测的高安全性的隐写算法设计, 取得了丰硕成果^[1]。然而, 数字隐写模型的研究未能同步进行。数字隐写模型的研究能够抽象隐写过程, 理清隐写术本质, 为隐写术的进一步研究提供支撑。

数字隐写模型的相关研究中, Costa 模型^[2]将秘密信息编码与载体叠加; Moulin 模型^[3]将秘密信息、密钥、载体作为编码的输入, 输出为完成嵌入的隐秘载体。与隐写模型相关的其他研究大多是基于隐写的通信系统模型, 如 Simmons 提出的经典的“囚徒问题”模型、刘静等^[4]建立的隐写博弈模型以及对抗博弈模型^[5]等, 这些是通过通信双方与攻击方的收益博弈来分析隐写安全相关的结论, 未将隐写的原理当作研究重点。Costa 模型与 Moulin 模型是直接描述数字隐写的模型, 描述隐写嵌入与提取过程的输入、输出、关键过程和目标要求。

Moulin 模型相对于 Costa 模型的优势在于其对密钥安全以及对失真限度的考虑, 成为后期描述隐写的经典模型。因此, Moulin 模型能够描述所有自适应隐写过程, 通用性强, 然而, 该模型无法准确描述具体的隐写方案, 用于描述目前主流的自适应隐写算法时, 不够准确。随着近年来高性能计算的发展、神经网络技术的发展, 出现了许多不同于传统意义上的隐写方案, 如利用生成对抗网络的隐写算法、半构造式隐写算法、完全构造式隐写算法等、基于载体选择与合成的隐写算法等^[6], 上述隐写模型已经无法描述这些新兴的隐写方案。

鉴于此, 本文梳理已有的隐写方案, 提出了通用数字隐写模型、基于载体修改的加性噪声隐写模型、最小化失真的数字图像自适应隐写模型, 并总结原理, 以指导隐写术的进一步研究。通用数字隐写模型描述当前的隐写过程; 基于载体修改加性噪声隐写模型, 描述当前实用的、主流的

隐写方案; 最小化失真的数字图像自适应隐写模型, 更加具体地描述通过定义失真与隐写编码来尽可能地减少对载体修改的隐写方案。3 个隐写模型间的关系如图 1 所示。

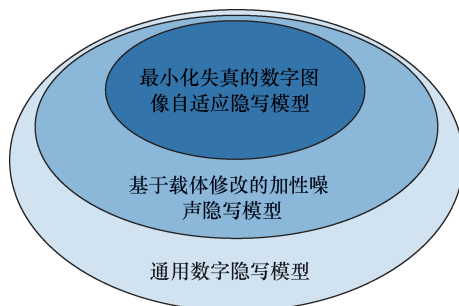


图 1 隐写模型间的关系
Figure 1 Relationships between steganography models

隐写模型共有的特征是：待传输的消息一定是隐写的一个输入项，隐写嵌入过程生成的必然是隐藏有消息的且具有逻辑意义的数字载体，隐写提取获得的必须是正确的消息。

2 通用数字隐写模型

隐写术的实质是将秘密消息“隐”式地“写”在某一特定形式的载体中。随着隐写术的发展, 多种隐写术的出现使原有载体模型的普适性不足。隐写术可分为 3 类：基于载体选择的隐写、基于载体生成的隐写、基于载体修改的隐写。以往研究的数字隐写通用模型适用于基于载体修改的隐写, 并不适用于前二者。为此, 本文提出通用的数字隐写模型。

通用数字隐写模型如图 2 所示。

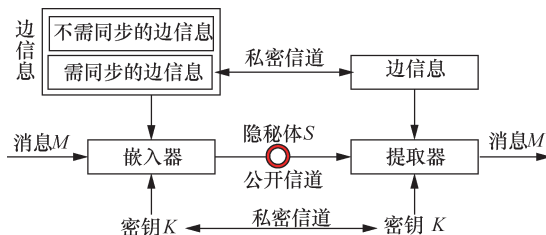


图 2 通用数字隐写模型
Figure 2 General digital steganography model

通用数字隐写模型可形式化描述为

$$\Gamma(M, K, SI_{\text{syn}}, SI_{\text{asy}}, ST, \text{Stego}, Em, Ex)$$

其中

1) M 为待隐写的秘密消息，多为 0-1 比特序列，也可以是图像等数字载体。其可以是经过收发双方共享的加解密密钥加密的密文，也可以是明文数据。

2) K 为隐写密钥。其作为随机数发生器的种子，用于提供隐写嵌入器生成隐秘载体必需的随机数。用于加解密消息的加解密密钥为隐写密钥的一部分。隐写密钥是隐写安全的最后一道防线，由收发双方在通信前或通信中在私密信道中采用某种方式协商共享。

3) ST 为隐写的约束条件。隐写的一个共同的约束条件是生成的隐秘体（集）具有一定逻辑意义、视觉上不可感知、具有一定抗检测能力。在某些隐写方案中存在失真代价的约束、嵌入率的约束等。

4) $Stego$ 为隐写嵌入后得到的隐秘体（集），多为数字媒体，能够隐藏在海量的数字媒体中。

5) Em 为隐写嵌入器具体操作， Ex 为隐写提取器具体操作。

6) SI_{syn} 为需同步的边信息， SI_{asy} 为不需要同步的边信息，二者统称为边信息。边信息指可用于对消息 M 进行编码的信息。边信息可分为需同步的边信息和不需同步的边信息。需同步的边信息，指收发双方需要通过私密信道事先同步的、用于准确提取消息的必要信息。不需同步的边信息，指发送方在嵌入器执行嵌入操作时需要使用的信息，接收方在提取信息时不需要该部分信息。比如，隐写采用的原始载体在大多数隐写方案中不需同步的边信息，而自适应隐写中的奇偶校验矩阵及秘密信息的长度需同步的边信息。

嵌入与提取过程为

$$Em(M, K, ST, SI_{syn}, SI_{asy}) \rightarrow Stego$$

$$Ex(Stego, K, SI_{syn}) \rightarrow M$$

嵌入器利用隐写密钥、同步的边信息以及嵌入过程必需的其他边信息，在约束条件的约束下，实现消息嵌入，生成隐秘体（集）。提取器利用隐写密钥和已同步的边信息，提取出消息。

3 基于载体修改的数字隐写模型

基于载体修改的数字隐写属于当前最常见的

数字隐写术。不论经典的最低有效位替换 LSB (least significant bit) 隐写、变换域隐写（如 JPEG 隐写），还是目前主流的空域自适应隐写算法 HUGO^[7]、HILL^[8]、MiPOD^[9]等，都是通过修改载体数据实现秘密消息的隐写。因此，对于基于载体修改的数字隐写模型研究具有重要意义，它是通用数字隐写模型的重要补充。

在基于载体修改的隐写的相关研究中（包括针对基于载体修改正向隐写的隐写分析技术），载体修改相当于将初始载体与表征具体嵌入修改模式（嵌入修改方式和嵌入修改位置）的一个向量进行叠加。这一修改向量是加性的，且叠加过程对载体造成了修改，可以形象地将该修改向量称为加性隐写噪声向量。加性隐写噪声的确定过程可能是非加性的（如采用非加性失真与隐写编码的隐写方案），而消息嵌入完成后生成的隐写噪声与初始载体的叠加过程，载体元素间以及隐写噪声元素间互不影响，可以直接进行叠加。因此，以加性隐写噪声为基础构建数字隐写模型，可以准确有效地描述基于载体修改的隐写，将这种模型称为基于载体修改的加性噪声隐写模型。Moulin 模型是一种简单的加性噪声隐写模型，但其用于描述图像空域自适应隐写中依据图像内容特征自适应确定嵌入修改模式时失效。加性噪声模型描述为在载体上叠加一层隐写噪声，可简单地记为

$$Stego = Cover + Noise$$

其中，Cover 为初始载体（集），Noise 为隐写嵌入生成的隐写噪声，Stego 为最终生成的隐秘体（集）。基于载体修改的加性噪声隐写模型如图 3 所示。

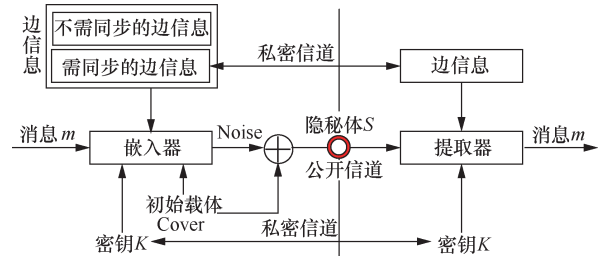


图3 基于载体修改的加性噪声隐写模型
Figure 3 Additive noise steganography model based on cover modification

基于载体修改的加性噪声隐写模型形式化描

述如下。

$$\Gamma(M, K, \text{Cover}, I, \text{ST}, \text{Noise}, \text{SI}_{\text{syn}}, \text{SI}_{\text{asy}}, \text{Stego}, \text{Em}, \text{Ex})$$

其中,

1) K 、 SI_{syn} 、 SI_{asy} 、 Stego 、 Em 、 Ex 符号含义同第2节。

2) M 在该模型中为 0-1 比特序列, 或者可以转换为 0-1 比特序列的数字载体。同样, 其可以是明文数据, 也可以是密文数据。

3) Cover 为初始载体, 其可以是文本、图像、语音、视频等数字媒体, 也可以是一些隐写数据的其他载体 (如网络协议、网络数据包等)。初始载体必须是离散的且具有固定的长度, 必须具备时间或空间上的冗余。

4) ST 仍表示隐写的约束条件。在该模型中, 初始载体被选定, 一个重要的隐写约束条件是初始载体与生成的隐秘体差距不能超过某一阈值 T , 即 $\text{diff}(\text{Cover}, \text{Stego}) \leq T$ 。

5) I 为嵌入修改方式集 (可作为需同步的边信息, 使收发双方准确同步), 若为 $\pm u (u > 0)$ 修改, 则对应的 $I = \{-u, \dots, -1, 0, +1, \dots, +u\}$ 。

6) Noise 为隐写噪声。Noise 是一个与初始载体和隐秘体具有相同规模的向量, $\text{Noise} = (I)_{n_1 \times n_2}$, $[n_1, n_2] = \text{sizeof}(\text{Cover}) = \text{sizeof}(\text{Stego})$ 。

从该模型出发讨论数字隐写, 数字隐写的关键是隐写噪声的确定。数字隐写的安全性取决于隐写噪声的特征, 隐写噪声对原始载体影响越小, 数字隐写的安全性越高。

嵌入与提取过程分别为

$$\text{Em}(M, K, \text{Cover}, I, \text{ST}, \text{SI}_{\text{syn}}, \text{SI}_{\text{asy}}) \rightarrow \text{Noise}$$

$$\text{Noise} \xrightarrow{\oplus \text{Cover}} \text{Stego}$$

$$\text{Ex}(\text{Stego}, K, I, \text{SI}_{\text{syn}}) \rightarrow m$$

4 最小化失真的数字图像自适应隐写模型

最小化失真的数字图像自适应隐写是基于载体修改隐写的一部分, 因图像载体易获得和足够复杂等特性, 以及图像隐写较高的隐写安全性, 成为当前研究的热点和难点。最小化失真的数字图像自适应隐写利用失真代价和隐写编码 (STC 码) 实现根据载体统计特征自适应确定嵌入修改模式 (嵌入修改位置和嵌入修改方式)。最小化失真的数字图像自适应隐写模型如图 4 所示。

在如图 4 所示的隐写模型中, 两项重要的内容是: 定义失真函数合理确定失真代价; 选择合理的隐写编码, 确定能使总体失真最小的隐写噪声。

最小化失真的数字图像自适应隐写模型可形式化描述为

$$\Gamma(M, K, \text{Cover}, I, L, \text{ST}, D, \text{Code}, \text{Noise}, \text{SI}_{\text{syn}}, \text{Stego}, f_{D1}, f_{D2}, \text{Em}, \text{Ex})$$

其中,

1) M 为待隐写的秘密消息, L 为嵌入过程中采用的轮数。在最小化失真的自适应隐写中, 通过采用失真代价更新和多轮嵌入进一步提升隐写的安全性。若只进行一次嵌入, 此时 $L=1$, 不需要对消息 M 进行分块; 否则, 需要将 M 按照一定的规则分成等长的 L 块。

2) 需同步的边信息 SI_{syn} , 包括嵌入修改方式

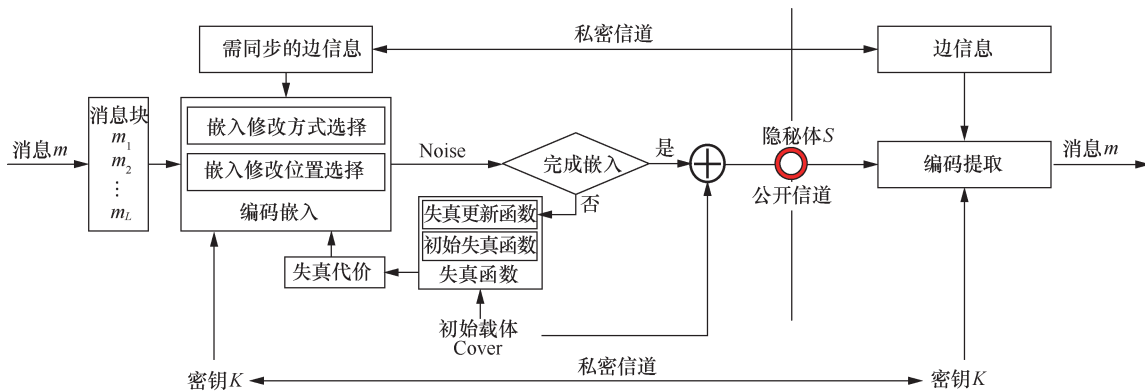


图4 最小化失真的数字图像自适应隐写模型

Figure 4 Digital image adaptive steganography model with minimal distortion

I 、轮数 L 、图像分块的方式、图像分块的扫描顺序、隐写编码必要的信息（秘密信息的长度、奇偶校验矩阵），以及其他隐写相关的必要信息。

3) ST 表示隐写的约束条件。在最小化失真的隐写中多采用失真受限的方式（另外讨论较多的是负载受限的方式），即失真代价的总和要满足一定的条件。

4) D 为失真代价，包含初始（首轮）失真代价 D_1 以及更新后第 $i(i \in [2, L])$ 轮的失真代价 D_i 。 f_{D1} 为初始失真函数， f_{D2} 为失真更新函数。 D 与 f_{D1} 、 f_{D2} 相互间的关系为

$$\begin{aligned} f_{D1}(\text{Cover}) &\rightarrow D_1 \\ f_{D2}(D_{i-1}, \text{Noise}, \text{Cover}) &\rightarrow D_i \end{aligned}$$

5) $Code$ 为采用的隐写编码方案，通过编码选择能够达到最小化失真要求的嵌入修改位置和嵌入修改方式。当前普遍采用的编码方案为 STC ，其为当前性能最优的隐写编码，具体过程可参照文献[10]和文献[11]。

嵌入与提取过程分别为

$$\begin{cases} f_{D1}(\text{Cover}) \rightarrow D_1 \\ \text{Em}(M, K, \text{Cover}, I, C, \text{Code}, D_i, SI_{\text{syn}}) \rightarrow \text{Noise} \\ f_{D2}(D_{i-1}, \text{Noise}, \text{Cover}) \rightarrow D_i \end{cases}$$

$$\text{Noise} \xrightarrow{\oplus \text{Cover}} \text{Stego}$$

$$\text{Ex}(\text{Stego}, K, I, \text{Code}, SI_{\text{syn}}) \rightarrow M$$

5 模型实例化描述

为了验证所提模型的有效性，分别选取 3 个典型的实例进行描述，采用通用数字隐写模型描述文献[12]中的深度隐写（deep steganography）和文献[13]中的无载体信息隐藏，采用基于载体修改的加性噪声隐写模型描述经典的 $LSBM$ 算法，采用最小化失真的数字图像自适应隐写模型描述文献[14]中的图像空域自适应隐写算法 $CMD-HILL$ 。

5.1 Deep Steganography

Baluja^[12]使用神经网络将全尺寸的彩色图像隐藏到另一幅相同尺寸的彩色图像中。采用深层神经网络实现隐写，采用另一神经网络（解码网络）实现秘密图像的提取。采用通用隐写模型描述，可写为

$$\Gamma_{\text{DeepStega}}(m_image, k, si_{\text{syn}}, si_{\text{asy}}, st, stego, Em, Ex)$$

模型的各参数为

$$m_image = [RGB]_{n_1 \times n_1} \in M;$$

$$k = \Phi \in K;$$

$$si_{\text{asy}} = \{\text{image_Cover}, \text{Prep_Network}, \text{Hiding_Network}\} \in SI_{\text{asy}}; // \text{分别表示载体图像、预处理网络、隐写网络}$$

$$si_{\text{syn}} = \Phi \in SI_{\text{syn}};$$

$$st = \text{error}(c, c', s, s') \in ST;$$

$$stego = [RGB]_{n_1 \times n_1} \in \text{Stego}$$

嵌入过程为

$$\text{Em}(m_image, k, si_{\text{syn}}, si_{\text{asy}}, st) \rightarrow stego$$

提取过程为

$$\text{Ex}(stego, k) \rightarrow m_image$$

由此可见，所提模型能够准确描述该深度隐写算法。

5.2 无载体信息隐藏

文献[13]中所提的无载体信息隐藏实质是一种基于载体选择的隐写。嵌入过程，构建文本信息关键词与图像特征的映射关系，搜索选择待隐写秘密消息对应的多幅图像作为隐秘体集，不对图像做任何处理；提取过程，根据所得隐秘载体集的图像特征和构建的映射关系，获得秘密消息片段，联接成秘密消息。采用通用隐写模型描述，可写为

$$\Gamma_{\text{CoverlessSteg}}(m, k, si_{\text{syn}}, si_{\text{asy}}, st, stego, Em, Ex)$$

模型的各参数为

$$m \in M; k \in K$$

$$si_{\text{asy}} = \{\text{image_database}\} \in SI_{\text{asy}}; // \text{表示图像库}$$

$$si_{\text{syn}} = \{\text{tag_sequence}, \text{mapping}\} \in SI_{\text{syn}}; // \text{分别表示标签序列和映射关系库}$$

$$st = \Phi \in ST;$$

$$stego = \{\text{image}_i, \dots, \text{image}_j, \dots\} \in \text{Stego}; // \text{image}_i, \text{image}_j \in \text{image_database}$$

嵌入过程为

$$\text{Em}(m, k, si_{\text{syn}}, si_{\text{asy}}, st) \rightarrow stego$$

提取过程为

$$\text{Ex}(\text{stego}, k) \rightarrow m$$

由此可见, 所提模型能够准确描述该无载体信息隐藏算法。

5.3 LSBM

LSBM 是经典的基于载体修改的隐写算法。采用第3节中的模型进行描述, LSBM 可写成

$$\Gamma_{\text{LSBM}}(m, k, c, e, \text{st}, \text{noise}, \text{si}_{\text{syn}}, \text{si}_{\text{asy}}, \text{stego}, \text{Em}, \text{Ex})$$

模型各参数为

$$m \in M;$$

$$[n_1, n_2] = \text{sizeof}(c);$$

$$c = \{\text{pixel}\}_{n_1 \times n_2} \in \text{Cover}, \text{pixel} \in [0, 255];$$

$$e = \{-1, 0, +1\} \in I;$$

$\text{st} = \{\text{payload} \leq 1\} \in \text{ST};$ //可以添加其他约束条件

$$\text{noise} = \{e\}_{n_1 \times n_2} \in \text{Noise};$$

$$\text{si}_{\text{syn}} = \{\text{sizeof}(m), e\} \in \text{SI}_{\text{syn}};$$

$$\text{si}_{\text{asy}} = \Phi \in \text{SI}_{\text{asy}};$$

$$\text{stego} = \{\text{pixel}\}_{n_1 \times n_2}$$

嵌入过程为

$$\text{Em}(m, k, c, e, \text{st}, \text{si}_{\text{syn}}) \rightarrow \text{noise} \xrightarrow{\oplus c} \text{stego}$$

提取过程为

$$\text{Ex}(\text{stego}, k, e, \text{si}_{\text{syn}}) \rightarrow m$$

由此可见, 所提模型能够准确描述 LSBM 隐写算法。

5.4 CMD-HILL

CMD-HILL^[14]由李斌等提出并实现, 属于隐写效果较优的最小化失真图像空域自适应隐写算法。采用最小化失真数字图像自适应隐写模型描述, 可写为

$$\Gamma_{\text{CMD-HILL}}(m, k, c, e, l, \text{st}, D_i, \text{code}, \text{noise}, \text{si}_{\text{syn}}, \text{stego}, f_{D1}, f_{D2}, \text{Em}, \text{Ex})$$

模型各参数为

$$m = \{m_1, m_2, m_3, m_4\} \in M;$$

$$[n_1, n_2] = \text{sizeof}(c);$$

$$c = \{\text{pixel}\}_{n_1 \times n_2} \in \text{Cover}, \text{pixel} \in [0, 255];$$

$$e = \{-1, 0, +1\} \in I;$$

$$l = 4 \in L;$$

$$\text{st} = \{\text{payload} \leq 0.5\} \in \text{ST};$$

$$\text{code} = \text{STC} \in \text{Code};$$

$$\text{noise} = \{e\}_{n_1 \times n_2} \in \text{Noise};$$

$$\text{si}_{\text{syn}} = \{H, \text{sizeof}(m), e, l\} \in \text{SI}_{\text{syn}};$$

$$\text{stego} = \{\text{pixel}\}_{n_1 \times n_2};$$

$$f_{D1}(c): D_1 = (d_{i,j})^{n_1 \times n_2} = \frac{1}{|c \otimes G| \otimes P_1} \otimes P_2;$$

$$f_{D2}(c, \text{noise}, D_{w-1}): D_w = \{\rho_{n_1 \times n_2}^+, \rho_{n_1 \times n_2}^-\}$$

$$\rho_{i,j}^+ = \begin{cases} \frac{d_{i,j}}{\alpha}, \sum_4 \text{noise}_{i,j} > 0 \\ d_{i,j}, \text{其他} \end{cases}$$

$$\rho_{i,j}^- = \begin{cases} \frac{d_{i,j}}{\alpha}, \sum_4 \text{noise}_{i,j} < 0 \\ d_{i,j}, \text{其他} \end{cases}$$

嵌入过程为

$$\text{Em}(m_1, k, c, e, \text{st}, \text{code}, D_1, \text{si}_{\text{syn}}) \rightarrow \text{noise}_1$$

$$\text{Em}(m_2, k, c, e, \text{st}, \text{code}, \text{noise}_1, D_2, \text{si}_{\text{syn}}) \rightarrow \text{noise}_2$$

$$\text{Em}(m_3, k, c, e, \text{st}, \text{code}, \text{noise}_2, D_3, \text{si}_{\text{syn}}) \rightarrow \text{noise}_3$$

$$\text{Em}(m_4, k, c, e, \text{st}, \text{code}, \text{noise}_3, D_4, \text{si}_{\text{syn}}) \rightarrow \text{noise}_4$$

$$\text{noise}_4 \xrightarrow{\oplus c} \text{stego}$$

提取过程为

$$\text{stego} \xrightarrow{l} \text{stego}_1, \text{stego}_2, \text{stego}_3, \text{stego}_4$$

$$\text{Ex}(\text{stego}_1, k, e, \text{code}, \text{si}_{\text{syn}}) \rightarrow m_1$$

$$\text{Ex}(\text{stego}_2, k, e, \text{code}, \text{si}_{\text{syn}}) \rightarrow m_2$$

$$\text{Ex}(\text{stego}_3, k, e, \text{code}, \text{si}_{\text{syn}}) \rightarrow m_3$$

$$\text{Ex}(\text{stego}_4, k, e, \text{code}, \text{si}_{\text{syn}}) \rightarrow m_4$$

$$m_1, m_2, m_3, m_4 \rightarrow m$$

由此可见, 所提模型能够准确描述 CMD-HILL 算法。

6 结束语

在梳理当前隐写算法、总结抽象数字隐写模型的过程中, 本文理清隐写术研究的几个关键点: 一是隐写嵌入过程的输入以及提取过程的输出,

要求必须是相同的秘密消息,这也是隐写研究的目标;二是嵌入得到的隐秘体,能够很好地隐藏在海量的数字载体中,在公开信道中能够避开攻击者的监测,这是隐写术研究的主要方向;三是利用隐写术实现隐蔽通信的关键是需同步的边信息的准确同步以及隐写密钥的共享。目前,研究主要集中于隐秘体的隐蔽性研究。在进一步的研究中,可继续开展隐秘体的隐蔽性研究,此外,可开展边信息的同步和密钥共享的研究,使隐写术走向实用。

参考文献:

- [1] HUSSAIN M. Image steganography in spatial domain: a survey[J]. Signal Processing: Image Communication, 2018, 65: 46-66.
- [2] COSTA M. Writing on dirty paper[J]. IEEE Transaction on Inform Theory, 1983, 29(3): 439-441.
- [3] MOULIN P, O'SULLIVAN J A. Information-theoretic analysis of information hiding[J]. IEEE Transactions on Information Theory, 2003, 49(3): 563-593.
- [4] 刘静, 汤光明. 大容量自适应隐写对抗的博弈研究[J]. 电子学报, 2014(10): 1963-1969.
LIU J, TANG G M. Game research on large-payload and adaptive steganographic counterwork[J]. Acta Electronica Sinica, 2014(10): 1963-1969.
- [5] LI J, YANG X, LIAO X, et al. A game-theoretic method for designing distortion function in spatial steganography[J]. Multimedia Tools & Applications, 2016: 1-15.
- [6] 张新鹏, 钱振兴, 李晟. 信息隐藏研究展望[J]. 应用科学学报, 2016, 34(5): 475-489.
ZHANG X P, QIAN Z X, LI S. Prospect of digital steganography research[J]. Journal of Applied Sciences-Electronics and Information Engineering, 2016, 34(5): 475-489.
- [7] PEVNY T, FILLER T, BAS P. Using high-dimensional image models to perform highly undetectable steganography[C]//12th International Workshop on Information Hiding. 2010: 161-177.
- [8] LI B, WANG M, HUANG J, et al. A new cost function for spatial image steganography[C]//IEEE International Conference on Image Processing. 2014: 4206-4210.
- [9] SEDIGHI V, COGRANNE R, FRIDRICH J. Content-adaptive steganography by minimizing Statistical detectability[J]. IEEE Transactions on Information Forensics & Security, 2015, 11(2): 221-234.
- [10] FILLER T, JUDAS J, FRIDRICH J. Minimizing embedding impact in steganography using trellis-coded quantization[C]//SPIE, Electronic Imaging, Media Forensics and Security XII, 2010: 18-20.
- [11] FILLER T, JUDAS J, FRIDRICH J. Minimizing additive distortion in steganography using syndrome-trellis codes[J]. IEEE Transactions on Information Forensics and Security, 2011, 6(3): 920-935.
- [12] BALUJA S. Hiding images in plain sight: deep steganography[C]//Advances in Neural Information Processing Systems. 2017: 2066-2076.
- [13] 周志立, 曹焱, 孙星明. 基于图像Bag-of-Words模型的无载体信息隐藏[J]. 应用科学学报, 2016, 34(5): 527-536.
ZHOU Z L, CAO Y, SUN X M. Coverless information hiding based on bag-of-words model of image[J]. Journal of Applied Sciences-Electronics and Information Engineering, 2016, 34(5): 527-536.
- [14] LI B, WANG M, LI X, et al. A strategy of clustering modification directions in spatial image steganography[J]. IEEE Transactions on Information Forensics & Security, 2015, 10(9): 1-14..

[作者简介]



宋海涛(1990-), 男, 山东烟台人, 信息工程大学博士生, 主要研究方向为信息隐藏、信息安全。



汤光明(1963-), 女, 湖南常德人, 信息工程大学教授、博士生导师, 主要研究方向为信息隐藏、信息安全。



孙怡峰(1976-), 男, 河南淇县人, 信息工程大学副教授, 主要研究方向为信息隐藏、人工智能。



王洋(1985-), 女, 陕西西安人, 信息工程大学博士生, 主要研究方向为网络与信息安全。