DOI: 10.3969/j.issn.0255-8297.2013.06.004

一种最优(k,p)进制转换算法

陈嘉勇[1,2,3], 张卫明[2], 胡金龙[2], 祝跃飞[2], 郭东辉[1]
1. 厦门大学 信息科学与技术学院, 福建 厦门 361005
2. 信息工程大学 网络空间安全学院, 郑州 450002
3. 中国科学院 信息安全国家重点实验室, 北京 100049

摘 要: 多进制编码和混合进制编码广泛应用于信息隐藏领域, 影响其编码性能的一个关键因素是进制转换效率. 针对任意 k 进制序列到 p 进制序列的相互转换, 提出一种高效的进制转换算法, 并根据信息论证明了其最优性. 利用新算法改进了 KT-Lex 文本隐写系统、网页等价标记隐写术、图着色编码和 APPM 编码等多种基于混合进制编码和分组多进制编码的隐写术, 有效提高了原方法的隐写性能. 理论分析和实验结果均表明了该算法的有效性.

关键词: 信息隐藏; 隐写术; 隐写编码; 转换效率; 嵌入效率; 嵌入容量
中图分类号: TP391 **文章编号:** 0255-8297(2013)06-0569-10

An Efficient (k,p) Notational System Transform Algorithm

CHEN Jia-yong[1,2,3], ZHANG Wei-ming[2], HU Jin-long[2], ZHU Yue-fei[2], GUO Dong-hui[1]
1. School of Information Science and Technology, Xiamen University, Xiamen 361005, Fujian Province, China
2. School of Cyberspace Security, Information Engineering University, Zhengzhou 450002, China
3. State Key Laboratory of Information Security, Graduate University of Chinese Academy of Sciences, Beijing 100049, China

Abstract: Muti-ary codes and mix-ary codes are widely used in information hiding, while the transfer efficiency between notational systems is an important factor of coding efficiency. An effective notational system transfer algorithm based on double-coding method is proposed for transforming arbitrary k-ary sequences to p-ary sequences. It is proved that the proposed notational system transform algorithm is optimal. The method is applied to improve embedding efficiency of several kinds of steganographic algorithms based on mix-ary codes or grouped multi-ary codes, including KT-Lex steganographic system, webpage steganography based on equal tag, grid coloring codes and APPM codes. Both theory analysis and experimental results show that the proposed method is effective.

Keywords: information hiding, steganography, steganographic coding, transform efficiency, embedding efficiency, embedding capacity

因特网的迅速发展对网络通信安全提出了越来越高的要求, 于是隐写术成为信息安全领域的一个研究热点. 隐写术是信息隐藏的重要分支, 它将秘密消息嵌入多媒体数据(如数字图像、音频、视频或文本) 中实现隐蔽通信. 这种数据嵌入技术不仅对于军事通信和国家信息安全有重要意义, 而且可用于电子商务、档案管理等领域. 隐写编码简称隐写码, 常用来提高隐写术的隐蔽性, 可以对载体做尽可能少的修改而嵌

收稿日期: 2011-09-02; **修订日期:** 2011-12-12
基金项目: 国家自然科学基金(No.60803155, No.60970141, No.60902102, No.61274133); 中国科学院战略性先导专项课题基金(No.XDA06030601); 国家重大科技专项基金(No.2 010ZX03004-003); 郑州市科技创新团队项目基金(No.10CXTD150)资助
作者简介: 陈嘉勇, 博士后, 研究方向: 网络安全, E-mail: cjy1003@sina.com; 祝跃飞, 教授, 博导, 研究方向: 密码学、网络安全; 郭东辉, 教授, 博导, 研究方向: 集成电路设计、人工智能、网络通信.

入尽可能多的信息[1]. 在隐写码的实际应用中，当待嵌信息为2进制信息而隐写信道为$p(p \neq 2)$进制信道或混合进制信道时，隐写者需要对消息进行进制转换. 消息进制转换效率是影响隐写术性能的重要因素.

根据隐写码所对应的隐写信道的进制差异可将隐写码分为3类：2进制隐写码、多进制隐写码和混合进制隐写码. 1) 2进制隐写码. 2进制隐写码的应用非常广泛，经典的最低有效位(least significant bit, LSB)替换即是一种2进制隐写码. 矩阵编码[2] 最早被提出来用以提高2进制隐写的嵌入效率，随后被用于著名的F5算法. 文献[3]提出了2进制隐写码的ZZW构造方法，可以从一个大嵌入率码出发生成一族嵌入率逐渐变小的码，并且可以证明：只要作为起点的大嵌入率码接近嵌入效率的上界，则随着嵌入率的减小，ZZW码族始终贴近嵌入效率效率上界. 后来，文献[4]证明了ZZW构造的渐进最优性. 因此，结合文献[5]的大嵌入率编码和ZZW构造可生成在各种嵌入率下接近最优的二元隐写码. 2) 多进制隐写码. 3进制隐写码是目前应用最广泛的多进制隐写码. 文献[6]指出, 采用LSB Matching的修改方式和3进制编码可获得最小的嵌入影响. 其中，LSB Matching即为一种经典的3进制隐写码. 文献[7-8]采用3进制Hamming码和3进制Golay码构造了性能优良的隐写码. 文献[9]针对载体数据修改方向的可选择性进行编码，提出EMD(exploiting modification direction)多进制隐写码，该方法可将3进制Hamming码作为特例. 随后，文献[10]基于图论方法提出了多进制图着色编码，文献[11]进一步提出了双次图着色编码. 3) 混合进制隐写码. 为使隐写算法具有更大的隐写容量或者更好的隐蔽性，部分学者通过对载体的不同位置定义不同嵌入失真，构造了混合进制隐写信道. 文献[12-14]分别以图像、音频和视频为载体，提出基于混合进制隐写信道的隐写算法. 此外，在基于语义的文本隐写术中，文本载体也经常被视为混合进制隐写信道. 例如：文献[15]提出的T-Lex系统可在具有同义词的单词中嵌入秘密信息，即该系统本质上采用了混合进制隐写技术. 文献[16]对T-Lex系统性能进行改进，并提出了KT-Lex系统. 文献[17]则提出了用网页等价标记置换技术在网页中隐藏信息的方法，本质上也是一种混合进制隐写术.

由于消息进制转换效率直接影响隐写术的实用性能，如何设计高效的进制转换编码算法是隐写术设计的关键问题之一，目前对该问题的研究成果较少. 对2进制序列与混合进制序列的相互转换问题，广泛采用文献[18]的方法，即通过将$\lfloor \mathrm{lb}\, p_i \rfloor$(其中，$\lfloor * \rfloor$表示对[*]向下取整)个2进制数编码为1个$p_i$进制数，可完成2进制到多进制序列或混合进制序列的相互转换. 对2进制序列与多进制序列的相互转换问题，文献[9]进一步提出了基于分组转换机制的进制转换算法，将2进制消息序列分为$\lfloor K\mathrm{lb}(2n+1) \rfloor$比特长的分组，用每个分组表示$K$个$(2n+1)$进制数. 该方法的转换效率高于文献[18]算法，但不适用于混合进制编码. 本文主要研究高效进制转换算法的设计、性能及应用.

1 符 号

隐写者拥有的消息源序列可以记为$\boldsymbol{m} = \{m_i\}^*$，欲得到的目标序列为$\boldsymbol{m}' = \{m_i'\}^*$. 记$e_{s\to d} = m/n$为将$s$进制序列转换为$d$进制序列的进制转换效率，其中，$m$为进制转换得到的目标序列的信息量，$n$为目标序列的信道容量. 显然，$0 \leqslant e_{s\to d} \leqslant 1$. 称$s$进制序列和$d$进制序列的相互转换问题为$(s,d)$进制转换问题.

多进制编码是指将2进制源序列$\boldsymbol{m}$与p进制目标序列$\boldsymbol{m}'$相互转换的编码方法，其中，$p \in \mathbf{N}$且$p \geqslant 3$. 混合进制编码指将2进制源序列$\boldsymbol{m}$与混合进制目标序列$\boldsymbol{m}'$相互转换的编码方法，其中，$\exists m_i' \in \boldsymbol{m}', m_j' \in \boldsymbol{m}'$，$m_i'$为$p$进制数，$m_j'$为$q$进制数，$p \geqslant 2, q \geqslant 2$且$p \neq q$. 特别地，多进制编码可视为混合进制编码的特殊情形.

在隐蔽通信中，假设欲传输的消息序列为2进制源序列$\boldsymbol{m}$，若发送方采用多进制隐写码(或混合进制隐写码)，则发送方需先将$\boldsymbol{m}$转换为多进制(或混合进制)的目标序列$\boldsymbol{m}'$，并利用嵌入算法将其嵌入载体中. 接收方利用提取算法从载体中提取消息$\boldsymbol{m}'$，然后将$\boldsymbol{m}'$转换为2进制序列$\boldsymbol{m}$, 具体流程如图1所示.

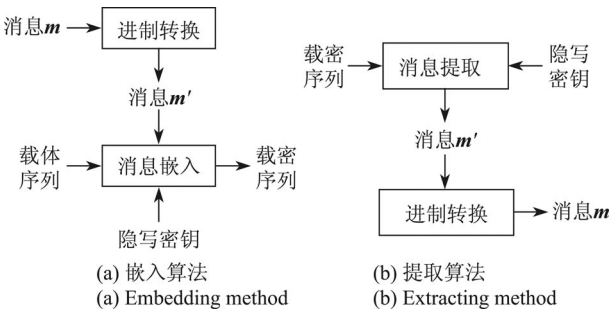

图 1 隐写通信流程

Figure 1 Steganographic communication process

下面给出通用的进制转换算法.

2 双层编码进制转换方法

考虑以下通用的进制转换问题：给定k进制源序列和$p(k < p)$进制目标序列，如何将k进制序列

与 p 进制序列相互转换?

2.1　优化双层编码算法

由于 $k<p$，故 $\exists t\in N$，且 $k^t\leqslant p<k^{t+1}$，$p=k^t+q(0\leqslant q<k^t)$. 下面给出 (k,p) 进制转换算法，本文称之为优化双层编码算法.

算法 1 (k,p) 优化双层编码算法. 计算编码参数 $\alpha=\frac{p-k^t}{k-1}$.

编码算法的步骤如下：

步骤 1　记源序列的前 $t+1$ 个元素为 $\{a_0,a_1,\cdots,a_t\}$，目标序列的第 1 个元素为 b_0，计算 $x=a_0k^t+a_1k^{t-1}+\cdots+a_t$，转至步骤 2.

步骤 2　若 $x<\alpha k$，则将 $t+1$ 个 k 进制数 $\{a_0,a_1,\cdots,a_t\}$ 编码为 $b_0=x$，返回步骤 1；否则，转至步骤 3.

步骤 3　若 $x\geqslant\alpha k$，计算 $y=a_0k^{t-1}+a_1k^{t-1}+\cdots+a_{t-1}$，将 t 个 k 进制数 $\{a_0,a_1,\cdots,a_{t-1}\}$ 编码为 $b_0=y+\alpha(k-1)=a_0k^{t-1}+a_1k^{t-1}+\cdots+a_{t-1}+\alpha(k-1)$. 由于 $\alpha\leqslant y\leqslant k^t-1$，$\alpha k\leqslant b_0\leqslant p-1$，返回步骤 1.

解码算法的步骤如下：

步骤 1　记待解码序列第 1 个元素为 b_0，计算 $b_0=a_02^t+a_12^{t-1}+\cdots+a_t$.

步骤 2　若 $b_0<\alpha k$，则将 b_0 解码为 $t+1$ 个 2 进制数 $\{a_0,a_1,\cdots,a_t\}$，返回步骤 1；否则，转至步骤 3.

步骤 3　计算 $b_0-\alpha(k-1)=a_02^{t-1}+a_12^{t-1}+\cdots+a_{t-1}$，将 b_0 解码为 t 个 2 进制数 $\{a_0,a_1,\cdots,a_{t-1}\}$，返回步骤3.

同理，对 $k>p$ 的情形，其编解码算法相当于 $k<p$ 情形的逆过程. 只需用算法 1 的解码算法进行编码，编码算法进行解码即可，这里不赘述.

特别地，当 $k=2$ 时，(2,p)优化双层编码算法的转换效率为

$$e_{2\to p}=\frac{\frac{2q}{2^{t+1}}(t+1)+\frac{2^{t+1}-2q}{2^{t+1}}t}{\mathrm{lb}\,p}=\frac{\lfloor\mathrm{lb}\,p\rfloor}{\mathrm{lb}\,p}+\frac{2p-2^{(\lfloor\mathrm{lb}\,p\rfloor+1)}}{2^{(\lfloor\mathrm{lb}\,p\rfloor+)}\mathrm{lb}\,p}\geqslant\frac{\lfloor\mathrm{lb}\,p\rfloor}{\mathrm{lb}\,p}$$

如(2,7) 进制转换和 (3,7) 进制的转换情况见表 1.

表 1　进制转换情况

Table 1　Value of notation system transfer

	进制转换情况							进制转换效率
(2,7) 进制转换	2 进制	000	001	010	011	100	101	11
	7 进制	0	1	2	3	4	5	6	$e_{2\to7}=0.979\,6$
(3,7) 进制转换	3 进制	00	01	02	10	11	12	2
	7 进制	0	1	2	3	4	5	6	$e_{3\to7}=0.941\,0$

2.2　进制转换性能分析

下面分析(k,p) 进制转换算法的进制转换效率和计算复杂度.

2.2.1　进制转换效率分析

文献 [18] 方法将 $\lfloor\log_k p\rfloor$ 个 k 进制数编码为 1 个 p 进制数，其 (k,p) 进制转换效率为

$$E_1=\frac{\lfloor\log_k p\rfloor}{\log_k p}$$

对优化双层编码而言，将 $\lfloor\mathrm{lb}\,m\rfloor+1$ 位进制数编码为 p 进制数的概率为 $kq/k^{\lfloor\mathrm{lb}\,m\rfloor}$，将 $\lfloor\mathrm{lb}\,m\rfloor$ 位 2 进制数编码为 p 进制数的概率为 $(1-kq)/k^{\lfloor\mathrm{lb}\,m\rfloor}$，故其 (k,p) 进制转换效率为

$$E_2=\frac{\frac{k\alpha}{k^{t+1}}(t+1)+\left(1-\frac{k\alpha}{k^{t+1}}\right)t}{\log_k p}=E_1+\frac{p-k^{\lfloor\log_k p\rfloor}}{(k-1)k^{\lfloor\log_k p\rfloor}\log_k p}$$

与文献 [18] 方法相比，优化双层编码的效率更贴近进制转换效率的上界，且满足

$$\lim_{\frac{p}{k}\to\infty}e_{k\to p}=1$$

即随着 p/k 的增大，优化双层编码的进制转换效率逐渐逼近上界 1.

当 $k=2$ 且参数 p 取不同值时，优化双层编码算法和文献 [18] 的进制转换效率对比情况如图 2 所示.

当参数 k 和 p 取不同值时，优化双层编码的 (k,p) 转换效率见图 3.

2.2.2　计算复杂度分析

记源序列的输入长度为 n，易知文献 [18] 的平均计算复杂度为 $C_1=O(n)$. 对优化双层编码方法而言，第 1 层编码的计算复杂度为 $O(n)$，第 2 层编码在最坏情况下的计算复杂度为 $O(n)$，且其平均计算复杂度为

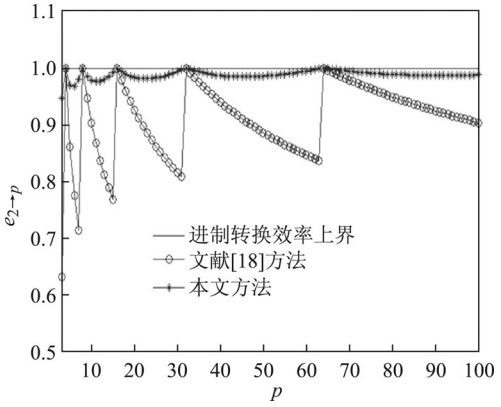

图 2　$(2,p)$ 转换效率的比较

Figure 2　Comparison of $(2,p)$ transfer efficiency

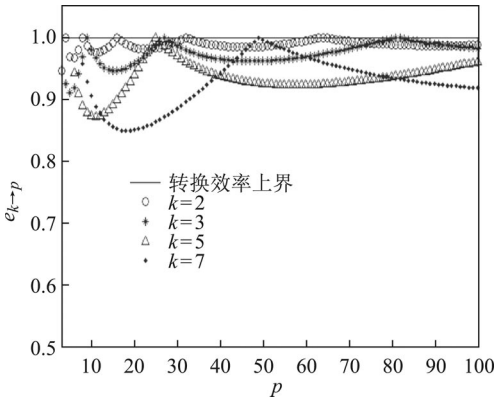

图 3 (k,p) 转换效率

Figure 3 (k,p) transfer efficiency

$$C_2=\left(2-\frac{p-k^{\lfloor\log_k p\rfloor}}{(k-1)k^{\lfloor\log_k p\rfloor}}\right)n$$

由于

$$n=C_1\leqslant C_2<2n \tag{1}$$

$$\frac{\lfloor\log_k p\rfloor}{\log_k p}=E_1\leqslant E_2$$
$$=\frac{\lfloor\log_k p\rfloor}{\log_k p}+\frac{p-k^{\lfloor\log_k p\rfloor}}{(k-1)k^{\lfloor\log_k p\rfloor}\log_k p} \tag{2}$$

综合2.2.1和2.2.2可知，优化双层编码是以牺牲较小的计算复杂度为代价而获得了较高的进制转换效率.

2.3 多进制分组编码问题

在混合进制隐写中，隐写者通常将 $x(x\geqslant 2)$ 个低进制的源序列信号转换为1个高进制的目标序列元素，这种机制称为非分组转换机制. 而在多进制隐写中，则允许先将 $x(x\geqslant 2)$ 个低进制的源序列信号转换为 $y(2<y\leqslant x)$ 个高进制的目标序列元素，这种机制被称为分组转换机制.

文献[9]提出了一种基于分组转换机制的进制转换方法，该方法用于多进制编码时进制的转换效率高于文献[18]，但不适用于混合进制编码. 文献[9]中的进制转换原理如下：把2进制消息序列分为 L bit 长的分组，再将每个分组转换为 K 个 $(2n+1)$ 进制数，其中

$$L=\lfloor K\mathrm{lb}\,(2n+1)\rfloor$$

该算法的进制转换效率为

$$e_{2\to(2n+1)}=\frac{L}{K\mathrm{lb}\,(2n+1)}$$

例如，对2进制序列 $\boldsymbol{m}=(1101\ 0110\ 1001)$，取 $L=4$，$K=2$，$\boldsymbol{m}$ 可转换为5进制序列 $(23\ 11\ 14)$，其转换效率为 $\frac{4}{2\times\mathrm{lb}\,5}=86.14\%$。

文献[9]提出的算法可推广至任意2进制序列 $\boldsymbol{m}$ 转换为 p 进制序列的情形. 首先将 $\boldsymbol{m}$ 按长度 L 分组，每个 L 长分组转换为 K 个 p 进制数, 其进制转换效率为

$$e_{2\to p}=\frac{L}{K\mathrm{lb}\,p}=\frac{\lfloor K\mathrm{lb}\,p\rfloor}{K\mathrm{lb}\,p}$$

随着 K 的增大，$e_{2\to p}$ 趋向于1，故该算法是一个渐进最优的进制转换算法. 在分组多进制转换的实际应用中，由于计算复杂度和载体的限制，分组长度只能取特定常数.

事实上，分组进制问题等价于将 2^L 进制序列转换为 p^K 进制序列，于是采用基于优化双层编码的 (k,p) 进制转换算法可完成该转换，则其进制转换效率为

$$e_{2^L\to p^K}=\frac{\lfloor\log_L p^K\rfloor}{\log_L p^K}+\frac{\log_L p^K-\lfloor\log_L p^K\rfloor}{2^{L(\lfloor\log_L p^K\rfloor+1)-1}\log_L p^K}$$

由于 $\lim\limits_{K\to\infty}e_{2^L\to p^K}=1$，故优化双层编码算法也是一种渐进最优的分组多进制编码算法.

在目标分组长度 K 和目标进制 p 不同的情形下，分别采用文献[9]和优化双层编码算法实现消息分组的多进制转换，所得结果见表2.

上述结果表明，优化双层编码的进制转换效率优于文献[9]方法，且分组长度越短，本文转换效率的优势越明显.

表 2 进制转换效率

Table 2 Notation system transfer efficiency

p	3			5			7			11		
L	3	4	6	4	6	9	5	8	11	6	10	13
文献[9]方法	0.946 3	0.841 2	0.946 3	0.861 3	0.861 3	0.969 0	0.890 5	0.949 9	0.979 6	0.867 1	0.963 5	0.939 4
本文方法	0.975 9	0.913 5	0.954 2	0.921 9	0.887 0	0.969 8	0.920 0	0.952 4	0.979 7	0.891 3	0.964 1	0.939 6

3　优化双层编码的最优性分析

进一步证明优化双层编码是最优进制转换编码算法.

不失一般性，假设n元字符集定义为$\boldsymbol{D}_m=\{0,1,\cdots,m-1\}$. 记源信号$s=\{s_i|s_i\in\boldsymbol{D}_2\}$为服从均匀分布的2进制随机变量序列. 目标信号$d$是$\boldsymbol{D}_m$上的随机变量，其概率密度函数为$d(x)$，信道容量为$C(d)$. 记$u$为$\boldsymbol{D}_n$上服从均匀分布的随机变量，则$u(x)=\frac{1}{|\boldsymbol{D}_n|}$为其概率密度函数.

定义编码$\boldsymbol{C}=\{\boldsymbol{C}(x)\}$为$\boldsymbol{D}_2$上有限长度的字符串集合，其中$\boldsymbol{C}(x)$为对应符号$x$的码字，令$l(x)$表示码字$\boldsymbol{C}(x)$的长度. 记$\boldsymbol{C}_{2\to m}$为$(2,m)$进制转换编码，则$\boldsymbol{C}_{2\to m}=\{\boldsymbol{C}(x)|x\in\boldsymbol{D}_m\}$，$\boldsymbol{C}_{2\to m}$将$l(x)$ bit长的2进制序列映射至m进制数x. 记x在目标信道出现的概率为$p(x)$，则有$p(x)=2^{-l(x)}$. $\boldsymbol{C}_{2\to m}$的进制转换效率$E(\boldsymbol{C}_{2\to m})=\frac{H(d)}{C(d)}$.

首先给出最优进制转换编码的定义.

定义1　$\boldsymbol{C}_{2\to m}$为最优$(2,m)$进制转换编码，则$\boldsymbol{C}_{2\to m}$满足

1) 覆盖性. $\boldsymbol{C}_{2\to m}$可将任意2进制序列$\boldsymbol{D}_2^{\#}$编码为m进制序列$\boldsymbol{D}_m^{\#}$.

2) 唯一可解性. $\boldsymbol{C}_{2\to m}$可将m进制序列$\boldsymbol{D}_m^{\#}$唯一解码为2进制序列$\boldsymbol{D}_2^{\#}$.

3) 最优性. $\boldsymbol{C}_{2\to m}$的进制转换效率$E(\boldsymbol{C}_{2\to m})$达到最大值.

引理1　$H(d)$满足$0\leqslant H(d)\leqslant \mathrm{lb}\ m$. 当且仅当$d$服从均匀分布时，$H(d)$取最大值.

证明

首先，有$H(d)=-\sum\limits_x p(x)\log_x p(x)\geqslant 0$.

根据文献[19]的定理2.6.4，有

$$H(d)\leqslant \log_x|\boldsymbol{D}_m|=\log_x m$$

当且仅当d服从均匀分布时等号成立.

引理2　$E(\boldsymbol{C}_{2\to m})$满足$0\leqslant E(\boldsymbol{C}_{2\to m})\leqslant 1$. 当且仅当$H(d)$取最大值，即$D(d||u)$取最小值时，$E(\boldsymbol{C}_{2\to m})$取最大值.

证明

由于

$$\begin{aligned}0\leqslant D(d||u)&=\sum_x p(x)\mathrm{lb}\frac{p(x)}{u(x)}\\&=\sum_x d(x)\mathrm{lb}\frac{p(x)}{\frac{1}{m}}=\mathrm{lb}\ m-H(d)\end{aligned}$$

故当且仅当$H(d)$取最大值时，$D(d||u)$取最小值.

由于目标信道容量

$$C(d)=\max_d H(d)=\mathrm{lb}\ m$$

故

$$E(\boldsymbol{C}_{2\to m})=\frac{H(d)}{\mathrm{lb}\ m}$$

从而

$$0\leqslant E(\boldsymbol{C}_{2\to m})\leqslant 1$$

特别地，根据引理1可知：当d服从均匀分布时，$H(d)$取最大值$\mathrm{lb}\,m$, $D(d||u)$取最小值0，$E(\boldsymbol{C}_{2\to m})$取最大值1.

引理3　若$\boldsymbol{C}_{2\to m}$满足唯一可解性，则$\boldsymbol{C}_{2\to m}$满足$\sum\limits_x 2^{-l(x)}\leqslant 1$.

证明

根据文献[19]中定理5.5.1的McMillan推论可知，$\boldsymbol{C}_{2\to m}$是为唯一可解码，则$\boldsymbol{C}_{2\to m}$的所有码字长度$l(x)$满足Kraft不等式，即有

$$\sum_x 2^{-l(x)}\leqslant 1$$

引理4　$f(n)=-2^{-n}\ \mathrm{lb}\ 2^{-n}$是关于$n$的严格单调递减函数.

证明

由于$f(n)=-2^{-n}\ \mathrm{lb}\ 2^{-n}=n2^{-n}>0$，则

$$\frac{f(n+1)}{f(n)}=\frac{(n+1)2^{-(n+1)}}{n2^{-n}}=\frac{n+1}{2n}<1n\geqslant 2$$

故$f(n)$为严格单调递减函数，对应不同的n，其值如图4所示.

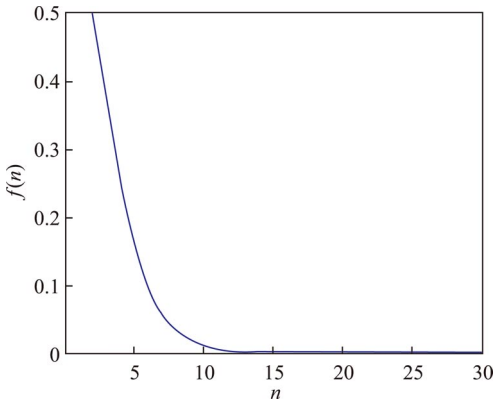

图4　$f(n)$取值

Figure 4　Value of $f(n)$

引理5　$\boldsymbol{C}_{2\to m}$为最优$(2,m)$进制转换编码，则$\boldsymbol{C}_{2\to m}$的理论最优码长为$\mathrm{lb}\ m$.

证明

$\boldsymbol{C}_{2\to m}$为最优$(2,m)$进制转换编码，则$D(d||u)$取最小值. 令

$$J=D(d||u)$$

则

$$J = \mathrm{lb}\, m - \sum_x p(x)\mathrm{lb}\, p(x)$$

当对 $\forall x$，$p(x)^* = \frac{1}{m}$ 时，J 取最小值 J^*.

由于 $\boldsymbol{C}_{2\to m}$ 将 $l(x)$ 比特长的 2 进制序列 $\boldsymbol{C}(x)$ 映射至 $x \in \boldsymbol{D}_m$，经 $\boldsymbol{C}_{2\to m}$ 编码后

$$p(x) = p\left(\boldsymbol{C}(x)\right) = 2^{-l(x)}$$

故对 $\forall x$，理论最优编码长度 $l(x)^*$ 为

$$l(x)^* = -\mathrm{lb}\, p(x)^* = \mathrm{lb}\, m$$

引理 6 在最优 $(2,m)$ 进制转换编码中，所有码长最长的码字成对出现，成对的最长码字仅在最后 1 bit 不同.

证明

首先，证明最优 $(2,m)$ 进制转换编码的最长码成对出现.

假设 $\boldsymbol{C}_{2\to m}$ 为最优 $(2,m)$ 进制转换编码且其最长码单独出现. 不失一般性，令 $x_0, x_1, x^* \in \boldsymbol{D}_m$，$\boldsymbol{C}_{2\to m}$ 中存在长为 $n+1$ 的最长码字 $\boldsymbol{C}(x_0) = \{s_0, s_1, \cdots, s_n, 0\}$，不存在 $\boldsymbol{C}(x^\star) = \{s_0, s_1, \cdots, s_n, 1\}$，$\boldsymbol{C}_{2\to m}$ 对应的目标信号的熵为 $H(d)$, 则 $\boldsymbol{C}(x_1)$ 的取值可分为以下两种情形：

情形 1 若 $\boldsymbol{C}(x_1) = \{s_0, s_1, \cdots, s_n\}$ 不是 $\boldsymbol{C}_{2\to m}$ 的码字，则保持其他码字不变，仅将码字 $\boldsymbol{C}(x_0)$ 改写为 $\boldsymbol{C}(x_0) = \{s_0, s_1, \cdots, s_n\}$，该作法不影响除 $\boldsymbol{C}(x_0)$ 和 $\boldsymbol{C}(x_1)$ 之外其他码字的编解码. 将新的编码方法记为 $\boldsymbol{C}^*_{2\to m}$，其对应的目标信号的熵记为 $H(d)^*$.

此时

$$\begin{aligned} H(d)^* &= -\sum_{x\neq x_0} p(x)\mathrm{lb}\, p(x) - p(x_0)\mathrm{lb}\, p(x_0) \\ &= -\sum_{x\neq x_0} p(x)\mathrm{lb}\, p(x) - 2^{-n}\mathrm{lb}\, 2^{-n} \end{aligned}$$

根据引理 4

$$\begin{aligned} H(d)^* &\geqslant -\sum_{x\neq x_0} p(x)\mathrm{lb}\, p(x) \\ &\quad - 2^{-(n+1)}\mathrm{lb}\, 2^{-(n+1)} = H(d) \end{aligned}$$

根据引理 2 可知，由于 $H(d)^* > H(d)$，故存在 $E(\boldsymbol{C}^*_{2\to m}) > E(\boldsymbol{C}_{2\to m})$，此时 $\boldsymbol{C}_{2\to m}$ 的最优性假设不成立.

情形 2 若 $\boldsymbol{C}(x_1) = \{s_0, s_1, \cdots, s_n\}$ 是 $\boldsymbol{C}_{2\to m}$ 的码字，则保持其他码字不变，仅将码字 $\boldsymbol{C}(x_1)$ 改写为 $\boldsymbol{C}(x_1) = \{s_0, s_1, \cdots, s_n, 1\}$，该作法不影响除 $\boldsymbol{C}(x_0)$ 和 $\boldsymbol{C}(x_1)$ 之外其他码字的编解码. 将新的编码方法记为 $\boldsymbol{C}^*_{2\to m}$，其对应的目标信号的熵记为 $H(d)^*$.

此时，由于 $\boldsymbol{C}(x_0)$ 和 $\boldsymbol{C}(x_1)$ 具有相同的前缀，编码时需优先编最长码 $\boldsymbol{C}(x_0)$. 若无法编码，再求次长码 $\boldsymbol{C}(x_1)$, 即有 $p(x_0) = p(x_1) = 2^{-n-1}$.

根据引理 4，此时

$$\begin{aligned} H(d)^* &= -\sum_{x\neq x_0,x_1} p(x)\mathrm{lb}\, p(x) - p(x_0)\mathrm{lb}\, p(x_0) \\ &\quad - p(x_1)\mathrm{lb}\, p(x_1) \\ &= -\sum_{x\neq x_0,x_1} p(x)\mathrm{lb}\, p(x) - 2^{-(n+1)}\mathrm{lb}\, 2^{-(n+1)} \\ &\quad - 2^{-(n+1)}\mathrm{lb}\, 2^{-(n+1)} \\ &\geqslant -\sum_{x\neq x_0,x_1} p\,(x)\mathrm{lb}\, p(x) - 2^{-(n+1)}\mathrm{lb}\, 2^{-(n+1)} \\ &\quad - 2^{-n}\mathrm{lb}\, 2^{-n} \\ &= H(d) \end{aligned}$$

根据引理 2, 由于 $H(d)^* > H(d)$, 存在 $E(\boldsymbol{C}_{2\to m^*}) > E(\boldsymbol{C}_{2\to m})$, 此时 $\boldsymbol{C}_{2\to m}$ 的最优性假设同样不成立.

结合情形 1 和 2 的结论可知，最优 $(2,m)$ 进制转换编码中所有码长最长的码字成对出现.

其次，证明最优 $(2,m)$ 进制转换编码中成对的最长码仅在最后 1 bit 特不同.

假设 $\boldsymbol{C}_{2\to m}$ 为最优 $(2,m)$ 进制转换编码，$\boldsymbol{C}(x_0)$ 和 $\boldsymbol{C}(x_1)$ 是成对的最长码字，两者的最后 2 bit 均不相同. 不失一般性，记 $\boldsymbol{C}(x_0)$ 和 $\boldsymbol{C}(x_1)$ 为 $\boldsymbol{C}(x_0) = \{s_0, s_1, \cdots, s_n, 0, 0\}$，$\boldsymbol{C}(x_1) = \{s_0, s_1, \cdots, s_n, 1, 1\}$，则保持其他码字不变，将码字 $\boldsymbol{C}(x_0)$ 改写为 $\boldsymbol{C}(x_0) = \{s_0, s_1, \cdots, s_n, 0\}$，将码字 $\boldsymbol{C}(x_1)$ 改写为 $\boldsymbol{C}(x_1) = \{s_0, s_1, \cdots, s_n, 1\}$, 将新的编码方法记为 $\boldsymbol{C}^*_{2\to m}$，其对应的目标信号的熵记为 $H(d)^*$.

此时根据引理 4 有

$$\begin{aligned} H(d)^* &= -\sum_{x\neq x_0,x_1} p\,(x)\mathrm{lb}\, p\,(x) - p\,(x_0)\mathrm{lb}\, p\,(x_0) \\ &\quad - p\,(x_1)\mathrm{lb}\, p\,(x_1) \\ &= -\sum_{x\neq x_0,x_1} p\,(x)\mathrm{lb}\, p\,(x) - 2^{-(n+2)}\mathrm{lb}\, 2^{-(n+2)} \\ &\quad - 2^{-(n+2)}\mathrm{lb}\, 2^{-(n+2)} \\ &\geqslant -\sum_{x\neq x_0,x_1} p\,(x)\mathrm{lb}\, p\,(x) - 2^{-(n+2)}\mathrm{lb}\, 2^{-(n+2)} \\ &\quad - 2^{-(n+2)}\mathrm{lb}\, 2^{-(n+2)} \\ &= H(d) \end{aligned}$$

根据引理 2, 由于 $H(d)^* > H(d)$, 存在 $E(\boldsymbol{C}^*_{2\to m}) > E(\boldsymbol{C}_{2\to m})$, 故最优 $(2,m)$ 进制转换编码中成对的最

长码仅在最后1 bit不同.

综上所述，引理6成立.

定理1　$(2,m)$优化双层编码是最优$(2,m)$进制转换编码.

证明

由于$l(x)\in\mathbf{N}$，结合引理5和6可得：$l(x)=\lceil \mathrm{lb}\, m\rceil$或$l(x)=\lfloor \mathrm{lb}\, m\rfloor$.

不失一般性，由于$x\in\boldsymbol{D}_m$，可根据$p(x)$的大小对$l(x)$进行重排序，使得

$$p(1)\leqslant p(2)\leqslant\cdots\leqslant p(m)$$

根据引理7可知：存在α，$0\leqslant 2\alpha\leqslant m$，使得

$$\begin{cases} l(1)=l(2)=\cdots=l(2\alpha)=\lceil \mathrm{lb}\, m\rceil \\ l(2\alpha+1)=l(2\alpha+2)=\cdots=l(m)=\lfloor \mathrm{lb}\, m\rfloor \end{cases}$$

由于$\boldsymbol{C}_{2\to m}$需满足唯一可解性，根据Kraft不等式有

$$\sum_{x=0}^{n-1}p(x)\leqslant 1$$

即

$$2\alpha\frac{1}{2^{\lceil \mathrm{lb}\, m\rceil}}+(m-2\alpha)\frac{1}{2^{\lfloor \mathrm{lb}\, m\rfloor}}\leqslant 1$$

$$\alpha\geqslant m-2^{\lfloor \mathrm{lb}\, m\rfloor} \tag{3}$$

由于$\boldsymbol{C}_{2\to m}$需满足覆盖性，即任取码字$D\in F_2^{\lfloor \mathrm{lb}\, m\rfloor}$，则$D$需满足①或者②：①$D\in\boldsymbol{C}_{2\to m}$，②$D||0\in\boldsymbol{C}_{2\to m}$且$D||1\in\boldsymbol{C}_{2\to m}$. 即$\boldsymbol{C}_{2\to m}$满足

$$2\alpha\frac{1}{2^{\lceil \mathrm{lb}\, m\rceil}}+(m-2\alpha)\frac{1}{2^{\lfloor \mathrm{lb}\, m\rfloor}}\geqslant 1$$

$$\alpha\leqslant m-2^{\lfloor \mathrm{lb}\, m\rfloor} \tag{4}$$

结合式(1)和(2)可得最优$(2,m)$进制转换编码的参数α满足

$$\alpha=m-2^{\lfloor \mathrm{lb}\, m\rfloor}$$

考虑本文第2节算法1，此时优化双层编码的编码参数$\alpha=\frac{m-2^{\lfloor \mathrm{lb}\, m\rfloor}}{2-1}=m-2^{\lfloor \mathrm{lb}\, m\rfloor}$，且码长为$2^{\lceil \mathrm{lb}\, m\rceil}$和$2^{\lfloor \mathrm{lb}\, m\rfloor}$的码字数量分别为$2\alpha$和$m-2\alpha$，故$(2,m)$优化双层编码是最优$(2,m)$进制转换编码.

定理2　(k,m)优化双层编码是最优(k,m)进制转换编码.

证明 同理可证，略.

4　优化双层编码的应用

相较现有的非分组进制转换(混合进制转换)和分组进制转换算法，优化双层编码方法具有更高的进制转换效率. 因此，优化双层编码可用以改进已有的涉及进制转换的算法和技术，如多进制、混合进制数字水印和数字隐写等. 下面以数字隐写术为应用背景，列举4个实例说明本文方法的有效性.

4.1　改进KT-Lex文本隐写系统

文本隐写术以文本为载体，利用文本在格式、编码、结构、语法和语义等方面的冗余，把隐秘信息隐藏到文本之中. T-Lex系统是由文献[15]提出的基于同义词替换的一个典型的文本隐写系统，采用WordNet中总共70 803个单词中的大约30%构成T-Lex系统中的同义词词典，并利用同义词的可选择性把给定的消息嵌入载体文本中. 同义词集合的大小平均为2.56，其中最大值、最小值分别为13和2. 文献[16]对T-Lex系统进行了改进并提出KT-Lex系统，其编码方案为：采用同义词替换，每替换一个同义词嵌入t bit信息，其中记n为同义词集合中的元素数目, 则$t=\lfloor \mathrm{lb}\, n\rfloor$.

对单个可用同义词替换的单词W_i，假设其同义词集合大小为n_i，原KT-Lex系统采用了文献[18]编码方案，W_i的隐藏容量为$C(W_i)=\lfloor \mathrm{lb}\, n_i\rfloor$.

若采用优化双层编码方案，则W_i的隐藏容量提高至

$$C(W_i)=\lfloor \mathrm{lb}\, n_i\rfloor+\frac{\mathrm{lb}\, n_i-\lfloor \mathrm{lb}\, n_i\rfloor}{2^{\lfloor \mathrm{lb}\, n_i\rfloor}}$$

下面用一个具体的例子简述上述的嵌入过程. 假设待嵌入的信息为$\boldsymbol{m}$=(0010 1100 1011 0010 1001$\cdots$)，发送方拥有的载体文本如下(其中右边上标表示同义词替换的位置序号)：

The new[1] booking system and priority[2] treatment[3] for local pregnant[4] women have the full support of private hospitals in Hong Kong. From February 1, mainland women suspected of entering Hong Kong to give birth will be asked[5] by immigration officers to furnish[6] their booking confirmation[7] certificates with local hospitals, Assistant Director of Immigration David Chiu said.

根据同义词词典，发送方找到第1个具有同义词的单词为“new”，其同义词集合为

$$\mathrm{Syn(new)}=\{\mathrm{new, fresh, novel, raw, newfangled, young}\}$$

采用优化双层编码算法的嵌入算法，可得每个同义词对应的编码消息为

$$\mathrm{Enc(new)}=\{\mathrm{new[000],\ \mathbf{young}[001],\ novel[010],\ raw[011],\ newfangled[10],\ fresh[11]}\}$$

由于发送信息的前3 bit为001，对应单词“young”，故可将“new”替换成“young”，从而嵌入3 bit消息.

同理，由于Enc(priority)={precedence[00], **priority**[01], antecedence[1]}；

Enc(treatment)={discussion[00], treatment[01], **discourse**[10], handling[11]}；

Enc(pregnant)={meaning[000], pregnant[001], **significant**[010], fraught[001]，momentous [10], important[11]}；

Enc(ask)={ask[000], inquire[001], enquire[010], require[011], expect[100], necessitate[10], **need**[11]}；

Enc(furnish)={supply[000], **provide**[001], render[01], furnish[10], give[11]}；

Enc(confirmation)={confirmation[00], **verification**[01], substantiation[1]}.

根据优化双层编码算法的嵌入规则分别将上面6个同义词嵌入消息分组01、10、010、11、001和01，全文本段共可嵌入17 bit消息.

消息嵌入后的文本段如下：The **young**[1] booking system and **priority**[2] **discourse**[3] for local **significant**[4] women have the full support of private hospitals in Hong Kong. From February 1, mainland women suspected of entering Hong Kong to give birth will be **need**[5] by immigration officers to **provide**[6] their booking **verification**[7] certificates with local hospitals, Assistant Director of Immigration David Chiu said.

接收方可按照优化双层编码的解码算法提取嵌入消息.

按照KT-Lex隐写系统采用的编码方法可得上述文档的隐藏容量为12 bit. 采用优化双层编码算法后，文本隐藏容量为17 bit，嵌入容量较原算法提高41.67%. 因此，本文方法可以有效改进KT-Lex隐写系统.

4.2 改进网页等价标记隐写术

网页隐写术以网页为载体，其原理主要可分为3类：基于不可见字符方法、基于标记大小变化方法和基于属性对顺序方法. 文献[17] 针对现有的网页信息隐藏技术存在隐蔽性差的缺点，弥补了基于属性对顺序的网页信息隐藏技术隐藏量小的缺陷，并提出一种基于等价标记的网页信息隐藏算法. 该算法采用等价标记置换原标记的方法来隐藏信息，具有较大的隐藏容量和较好的隐蔽性. 由于该方法本质上也是一种混合进制编码，故可用优化双层编码算法改进其嵌入效率.

记单个网页标记T_i的属性数目为n_i，则其能隐藏的最大信息量为$C(T_i)=\lfloor \mathrm{lb}\,(n_i!)\rfloor$. 采用优化双层编码方案后，$T_i$的最大隐藏容量为

$$C(T_i)=\lfloor \mathrm{lb}\,(n_i!)\rfloor+\frac{\mathrm{lb}\,(n_i!)-\lfloor \mathrm{lb}\,(n_i!)\rfloor}{2^{\lfloor \mathrm{lb}(n_i!)\rfloor}}$$

采用文献[18]和优化双层编码算法分别实现了基于等价标记的网页隐写术，并从Internet上下载www.yahoo.com、www.microsoft.com、www.ebay.com等主流网站的页面，进行网页隐藏容量测试. 采用优化双层编码后，网页隐写术的隐藏容量显著增长，实验结果见图5.

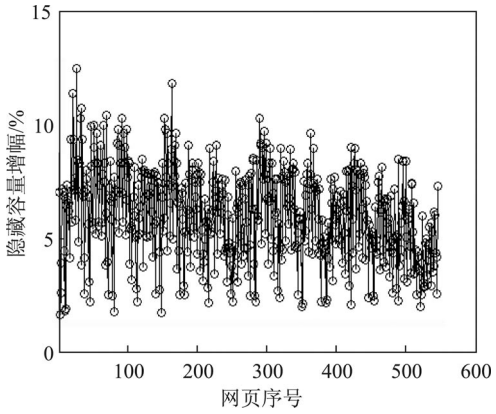

图 5 网页隐藏容量

Figure 5 Hiding capacity of webpages

实验结果表明，文献[18]和本文方法均能保持网页在浏览器上的正常浏览效果，而采用本文方法能有效提高文献[18]的隐藏容量，平均提高幅度约为7%.

4.3 改进图着色编码

下面以图着色编码为例，分析优化双层编码算法对分组多进制编码的改进性能. 图着色编码是由一种编码方法[10]，可在g个载体样本中嵌入1个$(2g+1)$进制数，其性能不低于Hamming隐写码的直和. 事实上，此方法的最早形式由文献[9]提出，称为EMD方法.

不妨取目标进制$p=3$，源序列分组长度$L=7$，目标序列分组长度$K=3$. 采用文献[9]方法和优化双层编码方法进行实验，结果见图6.

实验结果表明，在分组长度较短的情形下，相较于原始分组多进制编码，采用优化双层编码方法可有效提高多进制隐写码的实际嵌入效率. 事实上，上述改进不仅适用于图着色编码，而且对三元Golay隐写码和三元Hamming隐写码等其他多进制编码同样有效.

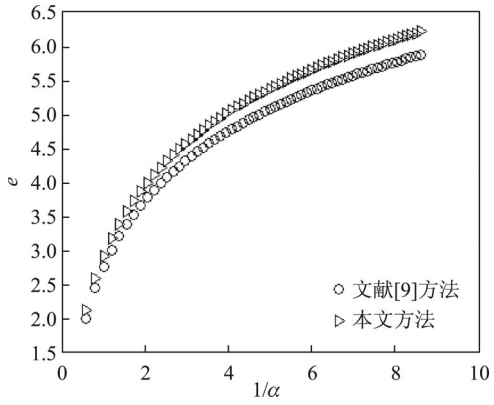

图 6　嵌入效率的比较

Figure 6　Comparison of embedding efficiency

4.4　改进 APPM 编码

文献 [20] 提出了基于像素对嵌入的 APPM (adaptive pixel pair matching) 隐写编码算法，该算法能适用于多种不同嵌入载荷且具有低嵌入失真的情形. 相较于早期的 LSB Matching 算法、EMD 算法和 DE(diamond encoding)算法，该方法具有多样的嵌入载荷，且在相同的载荷下具有相等或者更低的嵌入失真.

在混合进制条件下，将文献 [18] 中的算法和双层编码算法分别用于 APPM 算法的消息编码，考察本文算法的有效性. 这里采用 t_{MSE}(mean square error, MSE)来度量图像在嵌入消息后由于数据改变而引起的失真程度

$$t_{\mathrm{MSE}}=\frac{1}{M\times M}\sum_{i=0}^{M}\sum_{j=0}^{M}(p_{i,j}-p'_{i,j})$$

式中，$M\times M$ 表示图像的大小，$p_{i,j}$ 和 $p'_{i,j}$ 分别表示原始图像的像素值和载密图像的像素值. 实验结果见图 7.

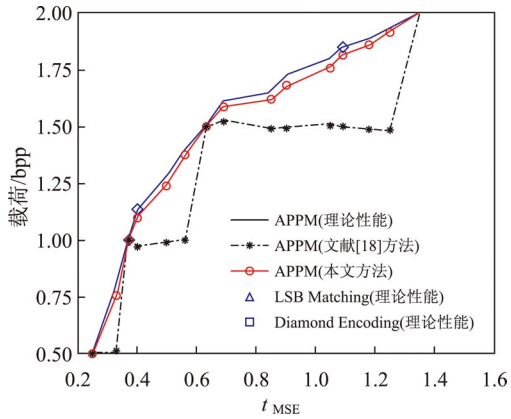

图 7　嵌入载荷的比较

Figure 7　Comparison of embedding payload

实验结果表明，在相同载荷条件下，优化双层编码可有效降低 APPM 算法的失真，进而提高该算法的整体性能.

5　结　语

对于采用多进制编码或混合进制编码的隐写术，消息的进制转换效率是影响其隐写性能的关键因素. 本文提出一种高效的进制转换编码算法，给出了任意 k 进制序列到 p 进制序列的相互转换方法，分析其性能并证明其最优性. 利用新算法对混合进制多进制隐写术进行改进，提高了多种隐写方法的嵌入容量或嵌入效率. 理论分析和实验结果均表明，优化双层编码算法是一种高效率的进制转换算法. 事实上，优化双层编码不仅应用于多进制隐写术和混合进制隐写术，而且对信道编码、数字水印等相关技术领域同样具有一定的参考价值.

参考文献:

[1] Zhang Weiming, Zhu Xuexiu. Improving the embedding efficiency of wet paper codes by paper folding [J]. IEEE Singal Processing Letters, 2009, 16(9): 794-797.

[2] Crandall R. Somes notes on steganography. posted on steganography mailing list [EB/OL]. http://os.inf.tu-dresden.de/~westfeld/crandall.pdf.

[3] Zhang Weiming, Zhang Xinpeng, Wang Shuozhong. Near-optimal codes for information embedding in gray-scale signals [J]. IEEE Transactions on Information Theory, 2010, 56(3): 1262-1270.

[4] Frtdrich J. Asymptotic behavior of the ZZW embedding construction [J]. IEEE Transactions on Information Forensics and Security, 2009, 4(1): 151-154.

[5] Frtdrich J, Soukal D. Matrix embedding for large payloads [J]. IEEE Transactions Information Security and Forensics, 2006, 1(3): 390-394.

[6] Frtdrich J. Minimizing the embedding impact in steganogaraphy [C]//Proccessing ACM the 8th Workshop on Multimedia and Security, 2006: 2-10.

[7] Dijk M V, Willems F. Embedding information in grayscale images [C]//Proccessing of 22nd Symposium on Information Theory, 2001: 147-154.

[8] Willems F, Dijk M V. Capacity and codes for embedding information in gray-scale signals [J]. IEEE Transations on Information Theory, 2005, 51(3): 1209-1214.

[9] Zhang Xinpeng, Wang Shuozhong. Efficient steganographic embedding by exploiting modification direction [J]. IEEE Communication Letters, 2006, 10(11): 67-70.

[10] Frtdrich J, Lisonek P. Grid coloring in steganography [J]. IEEE Transactions on Information Theory, 2007, 53(4): 1547-1549.

[11] Zhang Weiming, Zhang Xinpeng, Wang Shuozhong. Twice grid colorings in steganography [C]// Proccessing of 4th International Conference on Intelligent

Information Hiding and Multimedia Signal Processing, 2008: 1301-1304.

[12] 梁惠，郭立，陈运必. 基于视觉感知模型的大容量视频隐写算法 [J]. 中国科学院研究生院学报，2010(1): 55-62.
Liang Hui, Guo Li, Chen Yunbi. High capacity video steganographic algorithm based on visual perception model [J]. Journal of the Graduate School of the Chinese Acadamy of Sciences, 2010 (1): 55-62. (in Chinese)

[13] 耿广志，张汗灵，焦彩琼. 自适应的无损像素差分隐写算法 [J]. 计算机工程，2009, 35(23): 136-137.
Geng Guangzhi, Zhang Hanling, Jiao Caiqiong. Adaptive lossless pixel differencing steganographic algorithm [J]. Computer Engineering, 2009, 35(23): 136-137. (in Chinese)

[14] 郭志川，程义民，王以孝，谢于明. 一种无损的隐秘传输方法与仿真 [J]. 系统仿真学报，2006，18(6): 1638-1642.
Guo Zhichuan, Cheng Yimin, Wang Yixiao, Xie Yuming. Method and simulation of lossless covert communication [J]. Journal of System Simulation, 2006, 18(6): 1638-1642. (in Chinese)

[15] Winstein K. Lexical steganography through adaptive modulation of the word choice hash [EB/OL]. http://alumni.imsa.edu/∼keithw/tlex.

[16] 陈志立. 语言隐写术的分析与设计研究 [D]. 合肥：中国科技大学，2009.
Chen Zhili. Analysis and design of text steganography [D]. Hefei: University of Science and Technology of China, 2009. (in Chinese)

[17] 孙星明，黄华军，王保卫，孙光，黄俊伟. 一种基于等价标记的网页信息隐藏算法[J]. 计算机研究与发展，2007,44(5): 756-760.
Sun Xingming, Huang Huajun, Wang Baowei, Sun Guang, Huang Junwei. An algorithm of webpage information hiding based on equal tag [J]. Journal of Computer Research and Development, 2007,44(5): 756-760. (in Chinese)

[18] 陈志立，黄刘生，余振山，杨威，陈国良. 基于双文本段的信息隐藏算法 [J]. 电子与信息学报，2009, 31(11): 2725-2730.
Chen Zhili, Huang Liusheng, Yu Zhenshan, Yang Wei, Chen Guoliang. An information hiding algorithm based on double text segments [J]. Journal of Electronics & Information Technology, 2009, 31(11): 2725-2730. (in Chinese)

[19] Thomas M, Thomas J. Elements of information theory [M]. [S.l]: Wiley-Interscience, 1991: 35-45.

[20] Wien H. A novel data embedding method using adaptive pixel pair matching [J]. IEEE Transactions on Information Forensics and Security, 2011(99): 1-10.

(编辑：秦 巍)