隐写术中矩阵编码的保密安全性

陈嘉勇，刘九芬，祝跃飞，张卫明
（解放军信息工程大学 信息工程学院，河南 郑州 450002）

摘 要：针对矩阵编码在隐写码和湿纸码中的应用，基于信息论模型研究矩阵编码在不同攻击条件下的保密安全性。在已知载体攻击条件下，给出矩阵编码的密钥疑义度、消息疑义度和密钥的唯一解距。在选择载密攻击条件下，指出只需 n 个差分方程组即可恢复矩阵编码的共享密钥。

关键词：信息隐藏；隐写术；隐写分析；矩阵编码；矩阵嵌入；湿纸码
中图分类号：TP309 **文献标识码**：A **文章编号**：1000-436X(2012)06-0174-06

Cryptographic secrecy of steganographic matrix encoding

CHEN Jia-yong, LIU Jiu-fen, ZHU Yue-fei, ZHANG Wei-ming
(Information Science and Technology Institute, PLA Information Science and Technology University, Zhengzhou 450002, China)

Abstract: Based on an information theory model, the cryptographic security of matrix encoding, which can be applied in steganographic codes or wet paper codes, under different attack conditions was studied. The cryptographic security about matrix encoding under the condition of known-cover attack with key equivocation, message equivocation and unicity distance of stego-key was presented. The result that n groups of differential equations could sufficiently recover the share key of matrix encoding under the condition of chosen-stego attack was pointed out.

Key words: information hiding; steganography; steganalysis; matrix encoding; matrix embedding; wet paper codes

1 引言

隐写术是信息隐藏的重要分支，其目的是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。隐写安全性问题作为隐写术的核心问题，已成为信息隐藏领域的研究热点之一。

隐写术的安全性包括隐蔽安全性和保密安全性(简称隐蔽性和保密性)。早期对隐写安全性的研究主要集中在对隐蔽性的研究。Cachin[1]最早从通信角度研究隐蔽性，其采用信息论模型定义了主动攻击者与被动攻击者，并首次区分了完善隐蔽和完善保密的概念。Hopper[2]则从密码学角度研究隐蔽性问题，在被动攻击假设下，从计算复杂度角度定义了隐蔽性。近年来，随着隐藏信息提取问题的提出，部分学者指出：隐写术不仅具有隐蔽性，同时也具有保密性。其中，Fridrich 等[3,4]从计算复杂度角度分析了隐藏信息的“难提取性”问题，指出攻击者若能独立进行提取攻击，则可将恢复嵌入明文的攻击复杂度由 $O(|K|\times|E|)$ 降至 $O(\max\{|K|,|E|\})$。其中 K 为隐写密钥空间，E 为加密密钥空间。后来，张卫明等[5]指出隐写术带来的“难提取性”本质上

收稿日期：2010-08-23；**修回日期**：2010-12-07
基金项目：国家自然科学基金资助项目(60803155,60970141,60902102,61170234)；国家高技术研究发展计划(“863”计划)基金资助项目(2007AA01Z471)；郑州市科技创新团队基金资助项目(10CXTD150)
Foundation Items: The National Natural Science Foundation of China(60803155,60970141,60902102,61170234);The National High Technology Research Program of China(863 Program) (2007AA01Z471); Zhengzhou Municipal Science and Technology Innovation Team Project (10CXTD150)

是一种保密性，即使经隐写术嵌入的数据是未加密的，只要隐写术自身具有较强的保密性，其在密码学意义上仍是安全的。

作为提高通信隐蔽性的一种有效方法，矩阵编码首先由 Crandall[6]提出，后来被应用于著名的 F5 算法[7]。矩阵编码对隐蔽性的提高主要体现在 2 个方面：一是在嵌入相同消息前提下，减少对载体的修改(提高嵌入效率)；二是避开在载体的敏感区域嵌入消息。其中，矩阵编码用于前者时一般称为隐写码，而用于后者时则称为湿纸码[8]。从隐蔽性方面考虑，嵌入效率是衡量矩阵编码性能的重要指标。随机线性矩阵编码被证明可以用来逼近嵌入效率理论上界，但因其计算复杂度过高而不实用。近年来，许多学者通过在嵌入效率和计算复杂度之间寻找合理折中，设计了嵌入效率较高且能快速实现的矩阵编码方案。2010 年，Filler 等[9]考虑了隐写者可能赋予载体不同的失真度量，基于线性卷积码提出在任意失真度量准则下均可达到最小平均失真的 STC(syndrome-trellis codes)矩阵编码方法。Sarkar 等[10]从抗主动攻击角度出发，结合重复累积码提出 ME-RA(matrix embedding-repeat accumulate)矩阵编码方法，该方法在保持较高嵌入效率的同时提高了嵌入算法的顽健性。

到目前为止，对矩阵编码保密性的研究还很少。2008 年，Regalia[11]采用信息论方法，研究了唯载密攻击条件下矩阵编码的保密性问题。随着隐写分析技术的发展，被动攻击者可能获得更强的攻击条件。张卫明[12]提出针对图像隐写术的提取攻击方法，其通过建立污染数据分布模型获得载体图像的有效估计，进而实现隐藏信息的有效提取。该方法本质上属于已知载体攻击。一般情况下，攻击者想获得原始载体是困难的，但被动攻击者常常能通过载体恢复技术得到与原始载体具有符合优势的“准”载体对象，进而通过已知载体攻击提取隐藏信息。因此，通信双方不得不考虑更强攻击条件下矩阵编码的保密性。本文在 Regalia 的工作基础上，进一步研究矩阵编码在已知载体攻击和选择载密攻击条件下的保密性。

2　问题描述

2.1　记号

令 Σ 是有限字母集，Σ^n 是 Σ 的序列，其长度为 n。记载体序列为 S，载密序列为 C，消息为 M，通信双方共享的密钥矩阵为 $\boldsymbol{K}$，发送方采用的嵌入位置选取方式为 T。熵记为 $H(\cdot)$，条件熵记为 $H(\cdot|\cdot)$，互信息记为 $I(\cdot;\cdot)$。

对无失真信道，信道容量定义为 $C=H(C|S)$。$H(C|S)-H(M)$称为隐藏冗余。消息传输率定义为 $R_m=H(M)/n$。一个隐写系统对于唯载密攻击条件下密钥的唯一解距定义为：使伪隐写密钥量的数学期望为零的隐密对象的最少个数。已知载体攻击条件下密钥的唯一解距定义为：使伪隐写密钥量的数学期望为零的载体和隐密对象组的最少组数。一个$[n,k]$矩阵编码 C 是 F_2^n 的一个线性子空间。

下面考虑如何利用矩阵编码在无失真多媒体信道中传输秘密消息。假设通信双方欲利用长度为 n 的二元载体序列 $s(s\in F_2^n)$ 中传递 $q$bit 消息 $m(m\in F_2^q)$，其中，$q\leqslant n$。发送方先通过编码映射把载体信号映射到二元载体序列 s；再选定密钥矩阵 $\boldsymbol{k}(k\in F_2^{q\times n})$，通过矩阵编码在 s 中嵌入 $q$bit 消息 m 得到载密序列 $c(c\in F_2^n)$；进而生成载密信号。接收方在获得载密信号后，通过解码映射得到载密序列 c；结合密钥 $\boldsymbol{k}$ 通过矩阵编码提取隐蔽消息 m，其中，$m=\boldsymbol{k}c(\mathrm{mod}2)$。例如，最常用的编码映射为取载体信号的 LSB (least significant bit)序列，其对应的解码映射是用载密序列替换载体信号的 LSB 序列。特别地，对于好的编码映射函数而言，载体序列 s 的 2^n 种取值是等概的。假设消息 m 是经过压缩的，则 m 的 2^n 种取值也是等概的。若 s 中所有 n 个位置都是允许修改的，则上述矩阵编码方案为基于矩阵编码的隐写码方案。若发送方需要考虑某些不允许修改的敏感位置，则上述方案为基于矩阵编码的湿纸码方案。密钥矩阵 $\boldsymbol{k}$ 是 $F_2^{q\times n}$ 上的伪随机矩阵，根据矩阵中 01 分布的差异[11]，其可分为标准置换密钥矩阵和 Bernoulli 密钥矩阵。

2.2　隐写码

隐写码可在长度为 n 的二元载体序列 s 上嵌入 q 比特信息 m，而至多修改 s 的 R bit 信息。

嵌入算法 $Emb()$为

$$Emb(s,m)=s+e(m-\boldsymbol{k}s)=c$$

提取算法 $Ext()$为

$$Ext(c)=\boldsymbol{k}c$$

其中，

$$\boldsymbol{k}c=\boldsymbol{k}s+\boldsymbol{k}e(m-\boldsymbol{k}s)=\boldsymbol{k}s+m-\boldsymbol{k}s=m$$

2.3 湿纸码

湿纸码可在载体的某些位置被限制修改的情况下嵌入信息，而接收者无需知道哪些位置是受限的即可提取信息。与隐写码方案不同之处在于，发送方只能通过修改载体中“干”的位置嵌入 m。

假设载体 $s=(s_1,\cdots,s_n)$中有 l 个位置允许修改(即“干”的位置)其余 $n-l$ bit 不允许修改(即“湿”的位置)。记允许修改载体位为$\{s\}_j$，$j\in L\subset\{1,2,\cdots,n\}$，$|L|=l$。发送方通过修改 s 中 q 个“干”的位置，将消息 m 嵌入 s，得到 c。其中 $q\leqslant l\leqslant n$，且满足

$$\boldsymbol{k}c=m \tag{1}$$

取 $v=c-s$，则

$$\boldsymbol{k}v=m-\boldsymbol{k}s \tag{2}$$

由于 s 中有 $n-l$ 个位置不允许修改，故 v 对应的 $n-l$ 个分量只能取 0，即 v 中只有 l 个不确定分量 v_j，$j\in L\subset\{1,2,\cdots,n\}$，其余的 $n-l$ 个分量 v_i $(i\notin L)$ 为零。故对所有 $i\notin L$，从 $\boldsymbol{k}$ 中去掉第 i 列，共去掉 $n-l$ 列，所得矩阵记为 $\boldsymbol{h}$，相应地在 v 中删去 $n-l$ 个列向量 v_i，$i\notin L$，记为 u。从而式(2)可改写为

$$\boldsymbol{h}u=m-\boldsymbol{k}s \tag{3}$$

其中，$\boldsymbol{h}$ 是 $q\times l$ 维矩阵，u 是 l 维向量。通过求解式(3)即完成湿纸码的编码。

载体湿率记为 $\alpha_{\text{wet}}=(n-l)/n$，其中，$0\leqslant\alpha_{\text{wet}}<1$。事实上，隐写码也可视为一种特殊的湿纸码，即 $\alpha_{\text{wet}}=0$ 的湿纸码。湿纸码嵌入率记为 $r_{\text{wet}}=q/l$，特别地，隐写码的嵌入效率为 q/n。

3 已知载体攻击

3.1 密钥疑义度

引理 已知载体攻击条件下，对湿纸码有下式成立：

$$I(T;K,C,S,M)\geqslant\phi(n,q)\geqslant 0$$

证明

考虑 $I(T;K,C,S,M)$。由于选位方式 T 与嵌入消息 M 均与密钥 K 无关(接收方提取消息并不需要知道 T)，故对于任意给定的载体 S，有：

$$I(T;K,C,S,M)=I(T;C,S)=H(T)-H(T\mid C,S)$$

其中，$H(T)=\sum_{t\in T}\Pr(\boldsymbol{t})\log\dfrac{1}{\Pr(\boldsymbol{t})}=\log C_n^q$。从而关于选位方式 T 的信息只能通过比较载密对象 C 和载体对象 S 之间的差异获得，即

$$\begin{aligned}H(T\mid C,S)&=\sum_{c,s}\Pr(c\oplus s)H(T\mid c\oplus s)\\&=\sum_{i=0}^{q}\Pr(w(c\oplus s)=i)H(T\mid w(c\oplus s)=i)\end{aligned}$$

由于 c 是 F_2^n 上随机序列，$c\oplus s$ 的 Hamming 重量为 $w(c\oplus s)$，故

$$\Pr(w(c\oplus s)=i)=\frac{C_n^iC_{n-i}^{q-i}}{\sum_{j=0}^{q}C_n^jC_{n-j}^{q-j}}=\frac{C_n^iC_{n-i}^{q-i}}{C_n^q\sum_{j=0}^{q}C_q^j}=\frac{C_n^iC_{n-i}^{q-i}}{C_n^q2^q}$$

$$H(T\mid w(c\oplus s)=i)=\log C_{n-i}^{q-i}$$

由于 $\sum_{i=0}^{q}\dfrac{C_n^iC_{n-i}^{q-i}}{C_n^q2^q}=1$，根据 Jensen 不等式，有：

$$\begin{aligned}H(T\mid c\oplus s)&=\sum_{i=0}^{q}\frac{C_n^iC_{n-i}^{q-i}}{C_n^q2^q}\log C_{n-i}^{q-i}\\&\leqslant\log\left(\frac{\sum_{i=0}^{q}C_n^iC_{n-i}^{q-i}C_{n-i}^{q-i}}{C_n^q2^q}\right)=\log\sum_{i=0}^{q}C_q^iC_{n-i}^{q-i}-q\end{aligned}$$

从而

$$\begin{aligned}I(T;K,C,S,M)&=H(T)-H(T\mid c\oplus s)\\&\geqslant q+\log C_n^q-\log\sum_{i=0}^{q}C_q^iC_{n-i}^{q-i}\phi(n,q)\end{aligned}$$

由于 $0\leqslant i\leqslant q$，由 Vandermonde 恒等式(即 $\sum_{i=0}^{n}C_n^iC_m^{k-i}=C_{n+m}^k$)

$$\begin{aligned}0&=q+\log C_n^q-\log\sum_{i=0}^{q}C_q^iC_{n-q}^{q-i}\leqslant\phi(n,q)\\&\leqslant q+\log C_n^q-\log\sum_{i=0}^{q}C_q^iC_n^{q-i}=q\end{aligned}$$

从而，$0\leqslant\phi(n,q)\leqslant I(T;K,C,S,M)$(注：上述 $\phi(n,q)$ 已化为最简形式)。

定理 1 已知载体攻击条件下，矩阵编码的密钥疑义度具有上界：

$$I(K;S,C)\leqslant[H(C\mid S)-H(M)]-\phi(n,q)$$

其中，$\phi(n,q)=q+\log C_n^q-\log\sum_{i=0}^{q}C_q^iC_{n-i}^{q-i}$，$I(K;S,C)$ 在 $q=\dfrac{n}{2}$ 处取极大值。

证明

首先，

$$H(C,K,M,T,S)=H(K,M,T,S)+\underbrace{H(C\mid K,M,T,S)}_{=0}$$
$$=H(K)+H(M)+H(S)+H(T) \quad (4)$$

其次，

$$H(C,K,M,T,S)=H(C)+H(S\mid C)+H(K\mid C,S)+\underbrace{H(M\mid K,C,S)}_{=0}+H(T\mid K,C,S,M)$$
$$=H(C)+H(S\mid C)+H(K\mid C,S)+H(T\mid K,C,S,M) \quad (5)$$

联立式(4)和式(5)，得：

$$H(K)+H(M)+H(S)+H(T)=H(C)+H(S\mid C)+H(K\mid C,S)+H(T\mid K,C,S,M)$$
$$[H(S)-H(S\mid C)]+[H(K)-H(K\mid C,S)]+[H(T)-H(T\mid K,C,S,M)]=H(C)-H(M)$$

由于

$$\begin{cases}I(C;S)=H(S)-H(S\mid C)\\ I(K;C,S)=H(K)-H(K\mid C,S)\\ I(T;K,C,S,M)=H(T)-H(T\mid K,C,S,M)\end{cases}$$

故

$$I(C;S)+I(K;C,S)+I(T;K,C,S,M)=H(C)-H(M)$$

根据引理，

$$I(K;C,S)=H(C)-H(M)-I(C;S)-I(T;K,C,S,M)$$
$$=H(C\mid S)-H(M)-I(T;K,C,S,M)$$
$$\leqslant[H(C\mid S)-H(M)]-\phi(n,q) \quad (6)$$

根据 $\phi(n,q)$ 的取值和式(6)，对于固定的 n (如图 1 所示，n=30 时)，有：

1) 当 $r\to 0$ 或 $r\to 1$ 时，密钥疑义度达到最大上界，该上界趋向隐藏冗余；

2) 当 $r\to 0.5$ 时，密钥疑义度达到最小上界。

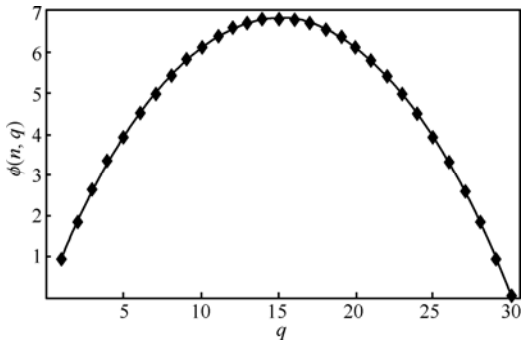

图 1　$\phi(n,q)$ 的取值情况

给定湿纸信道的湿率 α_{wet} ($\alpha_{\text{wet}}\neq 1$)后，湿纸码的消息嵌入率 r_{wet} 与密钥疑义度 $I(K;C,S)$ 具有如下关系。

1) 若 $0.5\leqslant\alpha_{\text{wet}}<1$，当 $r_{\text{wet}}=1$ 时，密钥疑义度最小；当 $r_{\text{wet}}\to 0$ 时，密钥疑义度最大，且接近隐藏冗余。

2) 若 $0\leqslant\alpha_{\text{wet}}<0.5$，当 $r_{\text{wet}}=\dfrac{1}{2(1-\alpha_{\text{wet}})}$ 时，密钥疑义度最小；当 $r_{\text{wet}}\to 0$ 时，密钥疑义度最大，且接近隐藏冗余。

3) 若 $\alpha_{\text{wet}}=0$，此时的湿纸码即为隐写码。当 $r_{\text{wet}}=0.5$ 时，密钥疑义度最小；当 $r_{\text{wet}}\to 0$ 时，密钥疑义度最大，且接近隐藏冗余。

定理 1 表明：为提高矩阵编码的保密性，应尽量减少隐藏冗余。在不同湿率条件下，通信双方可结合保密性需求与上述结论，选取合适的嵌入率。

3.2　消息疑义度

定理 2　已知载体条件攻击下，矩阵编码的消息疑义度具有上界：

$$I(M;S,C)\leqslant H(C\mid S)-[I(K;M,C)+\phi(n,q)]$$

其中，$\phi(n,q)=q+\log C_n^q-\log\sum_{i=0}^{q}C_q^iC_{n-i}^{q-i}$。对标准置换密钥模型：$I(K;M,C)=q-2^{-n}q$，对 Bernoulli 密钥模型：$I(K;M,C)\approx -2^{-n}nqH_2(p)$。

证明

$$I(M;S,C)=H(M)-H(M\mid S,C)$$

根据

$$H(C,K,M,T,S)=H(S)+H(C\mid S)+H(M\mid C,S)+H(K\mid M,C,S)+H(T\mid M,C,S,K) \quad (7)$$
$$H(C,K,M,T,S)=H(S)+H(K)+H(M)+H(T) \quad (8)$$

联立式(7)和式(8)，得：

$$H(M)-H(M\mid S,C)=H(C\mid S)+H(K\mid M,S,C)+H(T\mid M,C,S,K)-H(T)-H(K)$$
$$I(M;S,C)=H(C\mid S)-I(K;M,S,C)-I(T;M,C,S,K)$$

由于 $I(T;M,C,S,K)\geqslant\phi(n,q)$，$I(K;M,S,C)\geqslant I(K;M,C)$

$$I(M;S,C)\leqslant H(C\mid S)-I(K;M,S,C)-\phi(n,q)\leqslant H(C\mid S)-I(K;M,C)-\phi(n,q)$$

根据 Regalia[11]定理 2，对标准置换密钥模型，$I(K;M,C)=q-2^{-n}q$，故

$$I(M;S,C)\leqslant H(C\mid S)-q+2^{-n}q-\phi(n,q)$$

对 Bernoulli 密钥模型，$I(K;M,C)\approx 2^{-n}nqH_2(p)$，

故

$$I(M;S,C)\leqslant H(C\mid S)-2^{-n}nqH_2(p)-\phi(n,q)$$

其中，$p=\Pr(K_{ij}=1)=1-\Pr(K_{ij}=0)$。

定理 2 表明：对上述 2 种密钥模型，消息疑义度的上界均在嵌入率趋近于 0 时达到最大。

3.3 密钥的唯一解距

定理 3 已知载体攻击条件下，对采用固定密钥矩阵 $\boldsymbol{k}$ 的矩阵编码隐写方案，密钥 $\boldsymbol{k}$ 的唯一解距为

$$N\geqslant\frac{H(K)}{H(C\mid S)-[H(M)+I(T;M,C,S,K)]}$$

证明

记 N 个载体和载密分组对分别为 $s^N=\{s_1,s_2,\cdots,s_N\}$，$c^N=\{c_1,c_2,\cdots,c_N\}$。对给定的 N 个载体和载密对，所有可能的密钥组成的集合为

$$K(c^N,s^N)=\{\boldsymbol{k}\in K\mid\exists m_i\in M,t_i\in T,\ \text{满足}\Pr(m_i)>0\ \text{且}\ \boldsymbol{k}c_i=m_i\}$$

伪密钥数的数学期望为

$$\begin{aligned}\overline{K_p}&=\sum_{(c^N,s^N)\in(C^N,S^N)}\Pr(c^N,s^N)[K(c^N,s^N)-1]\\&=\sum_{(c^N,s^N)\in(C^N,S^N)}\Pr(c^N,s^N)K(c^N,s^N)-1\end{aligned}$$

由于

$$\begin{aligned}&H(K\mid c^N,s^N)\\&=\sum_{(c^N,s^N)\in(C^N,S^N)}\Pr(c^N,s^N)H(K\mid c^N,s^N)\\&\leqslant\log\sum_{(c^N,s^N)\in(C^N,S^N)}\Pr(c^N,s^N)\mid K(c^N,s^N)\mid\\&\leqslant\sum_{(c^N,s^N)\in(C^N,S^N)}\Pr(c^N,s^N)\mid K(c^N,s^N)\mid\\&=\log(\overline{K_p}+1)\end{aligned}$$

根据 $H(C\mid K,M,T,S)=0$，得：

$$\begin{aligned}&H(c^N,s^N,m^N,t^N,\boldsymbol{k})\\&=H(s^N,m^N,t^N,\boldsymbol{k})+\underbrace{H(c^N\mid s^N,m^N,t^N,\boldsymbol{k})}_{=0}\\&=N[H(S)+H(M)+H(T)]+H(K)\end{aligned}\tag{9}$$

故

$$\begin{aligned}&H(c^N,s^N,m^N,t^N,\boldsymbol{k})\\&=H(s^N)+H(c^N\mid s^N)+H(\boldsymbol{k}\mid c^N,s^N)+\\&\ H(m^N\mid c^N,s^N,\boldsymbol{k})+H(t^N\mid m^N,c^N,s^N,\boldsymbol{k})\\&\leqslant NH(S)+NH(C\mid S)+H(\boldsymbol{k}\mid c^N,s^N)+\\&\ H(t^N\mid m^N,c^N,s^N,\boldsymbol{k})\\&\leqslant N[H(S)+H(C\mid S)+H(T)-\\&\ I(T;M,C,S,K)]+H(\boldsymbol{k}\mid c^N,s^N)\end{aligned}\tag{10}$$

综合式(9)和式(10)，得：

$$\begin{aligned}H(\boldsymbol{k}\mid c^N,s^N)&\geqslant H(K)-N[H(C\mid S)-\\&\ H(M)-I(T;M,C,S,K)]\end{aligned}$$

从而

$$\begin{aligned}\log(\overline{K_p}+1)&\geqslant H(K)-N[H(C\mid S)-\\&\ H(M)-I(T;M,C,S,K)]\end{aligned}$$

伪密钥数的数学期望：

$$\overline{K_p}\geqslant H(\boldsymbol{k}\mid c^N,s^N)\geqslant 2^{H(K)-N[H(C|S)-H(M)-I(T;M,C,S,K)]}-1$$

密钥 $\boldsymbol{k}$ 的唯一解距：

$$N\geqslant\frac{H(K)}{H(C\mid S)-[H(M)+I(T;M,C,S,K)]}$$

4 选择载密攻击

定理 4 在选择载密攻击条件下，对采用固定密钥矩阵 $\boldsymbol{k}$ 的矩阵编码隐写方案，攻击者只需 n 个差分方程组即可恢复密钥 $\boldsymbol{k}$。

证明 从密码学角度分析，可将载体分组 s 看成明文，嵌入消息后的载密分组 c 看成密文，则明文和密文的分组长度均为 n。湿纸码可视为一个分组密码算法，其采用相同的密钥 $\boldsymbol{k}$ 加密多组不同的明文。假设攻击者事先已拥有大量明密对，则其可以选择需要的载密图像块 c 和对应的消息分组 m，这相当于做“选择密文”攻击。

在选择载密攻击条件下，下面给出一种恢复密钥 $\boldsymbol{k}$ 的差分攻击方法，其主要思路是：首先利用差分分析获得部分密钥信息，然后通过解线性方程组恢复密钥。以下运算均在 F_2 上讨论。

由于攻击者可选择密载密对象，故其可选 2 个载密对象分组 c_1 和 c_1'，它们仅在一个位置不同，即取 $c_1-c_1'=(1,0,0,\cdots,0)^{\mathrm{T}}$。设它们对应的明文消息分别为 m_1 和 m_1'，则可得差分方程组：

$$\boldsymbol{k}c_1-\boldsymbol{k}c_1'=m_1-m_1'$$

由于 $c_1-c_1'=(1,0,0,\cdots,0)^{\mathrm{T}}$，因此

$$\boldsymbol{k}(c_1-c_1')=\boldsymbol{k}_{j,1}=m_1-m_1'$$

同理，对 $c_i-c_i'=(0,0,\cdots\overset{i}{\overset{\frown}{1}},\cdots,0)^{\mathrm{T}}$，可得差分方

程组

$$\boldsymbol{k}_{j,i} = m_i - m_i'$$

其中，$i = 1,2,\cdots,n$。由于攻击者每次构造并求解一个差分方程组可获取关于 $\boldsymbol{k}$ 的 q bit 信息(一列信息)，故只需 n 个差分方程组即可恢复密钥 $\boldsymbol{k}$。

例如：在选择密文攻击条件下，攻击者欲恢复前述矩阵编码的密钥 $\boldsymbol{k} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}$，具体方法如下：首先，选取差分为 $(1,0,0,0)^{\mathrm{T}}$ 的任意 2 个载密对象，不妨取 $c_1 = (1,1,1,1)^{\mathrm{T}}$ 和 $c_1' = (0,1,1,1)^{\mathrm{T}}$。其次，取 2 个载密对象对应的明文消息，分别记为 $m_1 = (0,0,1)^{\mathrm{T}}$ 和 $m_1' = (1,1,1)^{\mathrm{T}}$。最后，计算 $m_1 - m_1' = (1,1,0)^{\mathrm{T}}$，$(1,1,0)^{\mathrm{T}}$ 即为密钥的第 1 列。同理，共用 4 个差分方程组即可完全恢复密钥 $\boldsymbol{k}$。

5　结束语

本文主要研究矩阵编码在不同攻击条件下的保密安全性。在已知载体攻击条件下，推导了矩阵编码的密钥疑义度、消息疑义度的理论界，给出了密钥的唯一解距；在选择载密攻击条件下，指出只需 n 个差分方程组即可恢复矩阵编码的密钥。本文研究结果表明，对采用固定共享密钥的矩阵编码而言，其在较强攻击条件下的保密性较差。如何通过控制矩阵编码共享密钥的生成方式以增强其抗已知载体攻击和选择载密攻击的能力，是值得进一步研究的问题。

参考文献：

[1] CACHIN C. An information-theoretic model for steganography[A]. Information Hiding 2nd International Workshop[C]. 1998. 306-318.

[2] HOPPER N. Toward a Theory of Steganography[D]. Pittsburgh: Carnegie Mellon University 2004.

[3] FRIDRICH J, GOLJAN M, SOUKAL D. Searching for the stego key[A]. Security, Steganography and Watermaking of Multimedia Contents[C]. 2004. 70-82.

[4] FRIDRICH J, GOLJAN M, SOUKAL D, *et al*. Forensic steganalysis: determining the stego key in spatial domain steganography[A]. Security, Steganography and Watermaking of Multimedia Contents[C]. 2005. 631-642.

[5] ZHANG W M, LI S Q, CAO J, *et al*. Information-theoretic analysis for the difficulty of extracting hidden information[J]. Wuhan University Journal of Natural Sciences, 2004, 10(1):315-318.

[6] CRANDALL R. Some notes on steganography[EB/OL]. http://os.inf.tudresden.de/. westfeld/crandall.pdf, 1998.

[7] WESTFELD R. F5-A steganographic algorithm[A]. Information Hiding 4th International Workshop[C]. 2001. 289-302.

[8] FRIDRICH J, GOLJAN M, LISONEK P, *et al*. Writing on wet paper[J]. IEEE Transactions on Signal Processing, 2005, 53(10):3923-3935.

[9] FILLER T, JUDAS J, FRIDRICH J. Minimizing embedding impact in steganography using trellis-coded quantization[A]. Proceedings of SPIE Electronic Imaging, Media Forensics and Security XII[C]. 2010. 1-14.

[10] SARKAR A, MADHOW U, MANJUNATH S. Matrix embedding with pseudorandom coefficient selection and error correction for robust and secure steganography[J]. IEEE Transactions on Information Forensics and Security, 2010, 5(2):225-239.

[11] REGALIA A. Cryptographic secrecy of steganographic matrix embedding[J]. IEEE Transactions on Information Forensics Security, 2008, 3(4): 786-791.

[12] 张卫明，李世取，刘九芬. 对空域图像 LSB 隐写术的提取攻击[J]. 计算机学报, 2007, 30(9):1625-1631.
ZHANG W M, LI S Q, LIU J F. Extracting attack to LSB steganography in spatial domain[J]. Chinese Journal of Computers, 2007, 30(9): 1625-1631.

作者简介：

陈嘉勇（1982-），男，福建厦门人，解放军信息工程大学博士生，主要研究方向为网络安全。

刘九芬（1963-），女，河南焦作人，解放军信息工程大学副教授、硕士生导师，主要研究方向为小波理论及其应用、信息隐藏。

祝跃飞（1962-），男，浙江杭州人，解放军信息工程大学教授、博士生导师，主要研究方向为信息安全、密码学。

张卫明（1976-），男，河北保定人，解放军信息工程大学副教授、硕士生导师，主要研究方向为信息隐藏、密码学。