文章编号: 1001-0920(2006)05-0572-04

随机调制隐写中的噪声同步分析

刘光杰, 戴跃伟, 王金伟, 王执铨
(南京理工大学 自动化系, 南京 210094)

摘 要: 针对Fridrich提出的使用固定密钥的随机调制算法, 提出一种基于噪声同步分析的隐写检测方法. 该方法使用图像复原、噪声估计和相关性计算实现对噪声同步程度的度量, 并对同步分析下随机调制隐写的安全容量进行了分析. 理论和实验表明, 固定隐写密钥的使用会降低随机调制算法的安全性.

关键词: 随机调制; 隐写分析; 噪声同步
中图分类号: TP273 **文献标识码**: A

On Noise Synchronization Analysis in Steganography Using Stochastic Modulation

LIU Guang-jie, DAI Yue-wei, WANG Jin-wei, WANG Zhi-quan
(Department of Automation, Nanjing University of Science and Technology, Nanjing 210094, China. Correspondent: LIU Guang-jie, E-mail: guangj_liu@yahoo.com.cn)

Abstract: A detection method is presented against the fixed-key-used stochastic modulation (SM) steganography proposed by Fridrich. The method uses image restoration, noise estimation and correlation calculation to realize the measure of the degree of noise synchronization. And under the noise synchronization analysis, the steganographic secure capacity is analyzed. Theory and experiments show that the use of fixed key will debase the security of stochastic modulation.

Key words: Stochastic modulation; Steganlaysis; Noise synchronization

1 引 言

隐写作为信息隐藏的一个重要的分支, 用于保护隐藏在载体中信息的安全性. 针对隐写的攻击称为隐写分析, 它是在已知或未知嵌入算法的情况下, 通过统计分析或模式分类等手段检测获得对象中是否存在秘密信息的技术. 由于在保障信息安全和提高隐写算法安全性方面的重要意义, 隐写分析已成为信息隐藏领域研究的热点.

隐写分析的研究开始于Westfeld对EzStego的χ^2分析, Provos在此基础上利用滑动窗机制扩展了Westfeld方法的应用范围; Fridrich[1]针对LSB嵌入给出了RS分析的检测方法, 并对基于JPEG图像的OutGuess和F5等算法进行了分析[2]; Dumitrescu[3]和张涛[4]等人也就空域LSB置换嵌入进行了研究. 另外Farid[5], Avcibas[6]等人从模式分类的角度对隐写分析进行了研究, 并给出未知嵌入算法情况下的通用检测算法.

某些文献同时也给出了一些具有更高安全性的隐写算法. 考虑到自然图像采集和处理过程存在的噪声, Marvel[7]提出一种以噪声掩盖秘密信息的扩频隐写方法(SSIS), 该方法通过将调制的经过纠错编码信息的高斯噪声添加到图像中, 实现了信息的隐藏, 但SSIS方法没有充分利用载体的信息, 而仅仅将其看作噪声, 因此平均每个像素上只能嵌入不到0.2个比特. 在此基础上, Fridrich[8]提出了一种称为随机调制(SM)的隐写算法, 该算法可将具有任

收稿日期: 2005-03-21; **修回日期**: 2005-06-27.
基金项目: 国家自然科学基金项目(60374066); 江苏省自然科学基金项目(BK2001054).
作者简介: 刘光杰(1980—), 男, 江苏徐州人, 博士生, 从事信息隐藏的分析理论与技术研究; 王执铨(1939—), 男, 武汉人, 教授, 博士生导师, 从事信息安全、动态大系统等研究.

意分布的 i i d 序列通过奇偶调制实现信息的隐藏. 由于该算法以调制噪声方式实现信息的嵌入, 而在统计上隐秘图像和自然含噪图像没有本质上的差别, 因此至今仍未见对此算法攻击的报道. 本文从多隐秘载体中的共有模式出发, 针对固定密钥的随机调制算法存在的噪声同步问题, 实现了对该算法多次使用后的隐写攻击.

2　随机调制隐写算法简述

随机调制算法中共使用 3 个密钥. K_1 用于加密具有双极性的二值序列 $b, b_i \in \{-1, 1\}$, 并产生 $m = \mathrm{Encrpt}(b, K_1)$; K_3 用于控制信息嵌入的随机游走, 载体序列 x 以密钥 K_3 置乱并产生置乱后的载体信号序列 $x' = \mathrm{Permute}(x, K_3)$; 密钥 $K_2 = [\mathrm{seed}, \sigma]$ 用以产生符合 $N(0, \sigma^2)$ 分布且经过取整运算的噪声序列 n.

单噪声的随机调制方法根据消息比特 m_i 和奇偶函数 $P(x, n)$ 输出的匹配性, 将噪声 n_i 加入 x_i 或从 x_i 中减去, 但由于取整后的高斯噪声包含较多的零, 而这部分噪声成分不能携带信息比特, 因此系统的容量仅为

$$C = 1 - \mathrm{erf}(1/2\sqrt{2}\sigma),$$
$$\mathrm{erf}(x) = \frac{2}{\sqrt{\pi}}\int \mathrm{e}^{-t^2}\mathrm{d}t \qquad (1)$$

为提高隐写容量, 文献[8]还介绍了一种基于双随机序列的随机调制方法. 用于调制信息的噪声序列 n^1, n^2 分别由 $K_{21} = [\mathrm{seed}_1, \sigma_1]$ 和 $K_{22} = [\mathrm{seed}_2, \sigma_2]$ 产生. 此时信息比特 -1, 1 分别对应着在 x_i 中加入 n_i^1 和 n_i^2. 此外, Fridrich 还讨论了根据要求的信息容量自适应选择噪声方差 σ^2 的方法, 通过自适应方差选择, 将所有信息比特分散在整个图像区域, 避免嵌入后的载体图像出现噪声不均匀现象.

在对称密钥机制下, 随机调制算法信息的准确提取依赖于发方和收方所持噪声序列的同步. 对于单噪声随机调制方法, 接收方需要知道 $K = [K_1, K_2, K_3]$, 其中 K_2, K_3 保证了噪声的同步. 对于双噪声调制, 接收方需要知道 $K = [K_1, K_{21}, K_{22}, K_3]$, 其中 K_{21}, K_{22}, K_3 保证了噪声的同步.

3　随机调制中的噪声同步分析

一般来说, 一个实用的保密通信系统不可能频繁改变事先约定好的密钥, 这是因为密钥的传输要求更可靠且更高的安全性. 在隐写密钥 K 固定的情况下, 若分析者可获得多个隐秘图像, 则可通过判断隐秘图像中包含噪声序列的同步性来判断通信双方是否存在隐写行为, 这是因为正常情况下, 图像处理和采集过程引入的噪声并不具有类似于随机调制的同步现象.

3.1　单噪声随机调制的同步分析

3.1.1　噪声方差固定的同步分析

设发送方 Alice 和接收方 Bob 在对称密钥机制下使用固定密钥, 以随机调制方法进行了多次秘密信息的传输, 攻击者 Wendy 可获得 N 个具有相同尺寸的隐秘图像 $S = \{s^1, s^2, \cdots, s^N\}$, 并设其对应的载体图像分别为 $X = \{x^1, x^2, \cdots, x^N\}$. 若第 i 个图像 s^i 的第 k 个像素携带了信息比特, 其应该具有如 $s_k^i = x_k^i \pm n_k$ 的形式.

由于单噪声调制只使用一个噪声序列且信息的嵌入以噪声加和减的形式给出, 因此当 $N = 2$ 时即可进行噪声同步性的分析. 为此首先利用 Wiener 滤波器得到 s 的复原图像 $\tilde{s}$,

$$\tilde{s}(i, j) = \mu + \frac{\sigma^2 - v^2}{\sigma^2}(s(i, j) - \mu),$$
$$\mu = \frac{1}{MN}\sum_{i,j\in\eta} s(i, j),$$
$$\sigma^2 = \frac{1}{MN}\sum_{i,j\in\eta} s^2(i, j) - \mu^2. \qquad (2)$$

式中: η 为像素 $s(i, j)$ 的 $M \times N$ 邻域, v^2 为所有邻域方差的均值. 由此可得估计的噪声序列 $n = s - \tilde{s}$. 然后利用如下相关公式计算隐秘图像 s^i 和 s^j 的估计噪声 $\hat{n}^i, \hat{n}^j$ 的相关性, 并以此度量两幅图像之间的同步性:

$$\mathrm{Corr}(X, Y) = \frac{\sum_i\sum_j (X_{ij} - \bar{X})(Y_{ij} - \bar{Y})}{\sqrt{\sum_i\sum_j (X_{ij} - \bar{X})^2 \cdot \sum_i\sum_j (Y_{ij} - \bar{Y})^2}}. \qquad (3)$$

设隐秘图像 s^i 和 s^j 中选择嵌入数据量的像素数和图像像素个数的比值分别为 p_i 和 p_j. 根据随机调制的原理, 由于在同一位置两幅图像对应的信息比特 m_i 和 x_i 的不同, 估计出的噪声序列 n^i, n^j 间将具有 $\min(p_i, p_j)/2$ 的相同符号的噪声成分, 和 $\min(p_i, p_j)/2$ 的相反符号的噪声成分. 因此在计算相关性时, 为避免噪声符号对相关性计算的影响, 可选择估计噪声 $\hat{n}$ 的绝对值来度量估计噪声的相关性, 即 $\mathrm{Corr}(|n^i|, |n^j|)$.

为判断两幅图像中是否存在噪声同步, 还需估计出正常情况下待分析的自然含噪图像所含噪声的相关程度. 这可通过轻微置乱估计噪声 n^j 并计算相关值 $\mathrm{Corr}(|n^i|, |SP(n^j)|)$ 来实现. 由于估计噪声中同时包含着图像本身的噪声成分, 轻微置乱应保证不破坏图像本身噪声的相关度, 因此本文使用如下置乱函数进行去同步的置乱:

$$P(n) = n', n_i' = n_{i-(-1)^i}, i = 1, \cdots, L. \qquad (4)$$

至此, 可定义两幅隐秘图像间的同步度量为

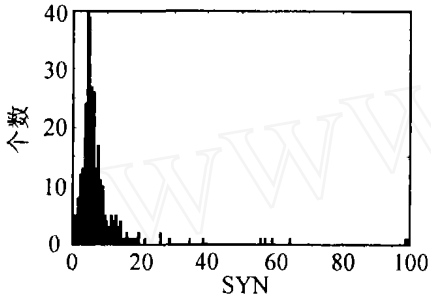
$$\mathrm{SYN}(s^i, s^j) = \left| \frac{\mathrm{Corr}(|n^i|, |n^j|) - \mathrm{Corr}(|n^i|, |P(n^j)|)}{\mathrm{Corr}(|n^i|, |P(n^j)|)} \right|. \quad (5)$$

通过比较 SYN 与阈值 Γ, 可检测出两幅图像是否存在着以随机调制方法嵌入的秘密信息:

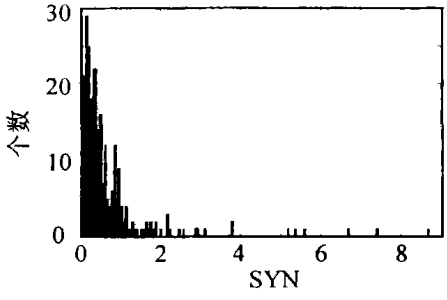
$$J = \begin{cases} \text{存在随机调制隐写}, & \mathrm{SYN} \geq \Gamma; \\ \text{不存在随机调制隐写}, & \mathrm{SYN} < \Gamma. \end{cases} \quad (6)$$

为保证算法具有较小的错误概率, 必须合理地选择阈值 Γ.

为此, 选择 800 幅 256 × 256 的灰度自然图像, 以方差 $\sigma^2 = 4$, 在所有像素上利用随机调制方法进行嵌入($p = 1$), 产生了以固定密钥调制了秘密信息的图像集合. 在此集合上, 计算其中任意 500 对隐秘图像 SYN 的分布情况, 如图 1(a) 所示. 为比较自然含噪图像的 SYN 分布情况, 将方差为 4 的随机高斯噪声加入此 800 幅图像中, 产生了含噪图像集合, 并检查其中任意 500 对含噪图像的 SYN 分布, 如图 1(b) 所示.



(a) 随机调制隐写图像的 SYN 值分布



(b) 随机加噪图像 SYN 值分布

图 1 800 幅图像集的 SYN 分布情况

从图 1 可以看出, 经过随机调制嵌入后, 任意两幅图像的 SYN 值小于等于 0.5 的概率为 6%, 而对随机加噪的自然图像小于等于 0.5 的概率为 89%, 因此选择阈值 $\Gamma = 0.5$. 实验发现, 对于更大方差的随机加噪图像, 任意两幅图像的 SYN 值依然大部分小于 0.5. 因此可认为, 阈值 0.5 能较好地区分自然含噪图像和随机调制隐写产生的含噪图像. 实验同时发现, 随着隐写使用的方差的减小, 估计噪声中同步的成分也越来越少, SYN 值的分布也趋于自然含噪图像的分布, 此时检测器不能很好地检测出隐写的存在.

在同步分析的攻击下, 若隐写双方不希望被检测器发现随机调制隐写的存在, 则必须调整嵌入使用的方差, 而方差的改变必然影响系统的隐写容量. 于是对 512 × 512 的灰度图像 Lena 和 Jet 进行了实验, 分别以 $\sigma^2 \in [0.1, 3]$ 进行随机调制隐写, 并以式 (6) 给出的同步检测公式进行检测. 结果表明, 不引起检测器发现的最大安全容量为

$$C_{\max} = \max(\min(p_1, p_2))\left(1 - \mathrm{erf}\left(1/2\sqrt{2\sigma}\right)\right), \quad (7)$$

其中 p_1 和 p_2 分别表示选择嵌入数据量的像素数和图像总像素个数的比值. 图 2 给出了不同方差下的理论最大容量以及最大安全容量. 当 σ^2 超过 0.5 时, 安全容量快速衰减; 当 $\sigma^2 = 3$ 时, 安全通信容量降低至 0.073 2. 从图中可以看到, 对于 Lena 和 Jet 而言, 系统可能取得的最大安全容量为 0.483 8, 并在 $\sigma^2 = 0.5$ 处取得.

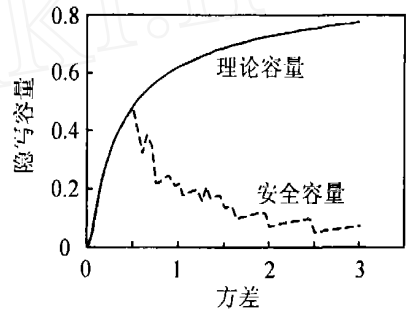


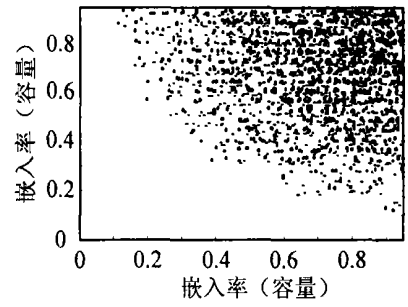
图 2 Lena 和 Jet 的理论容量和安全容量的比较

3.1.2 自适应选择 σ^2 情况下的噪声同步分析

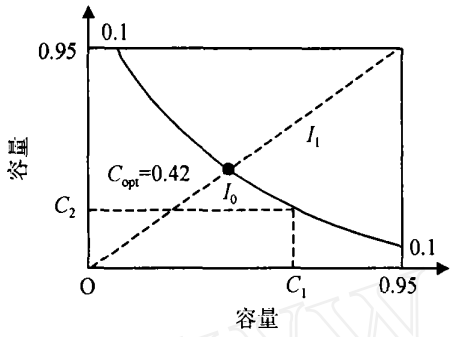
根据式(1), 若系统需要嵌入的数据量为 C, 则可自适应地选择噪声方差 $\sigma = \sqrt{2}/4\mathrm{erf}^{-1}(1 - C)$, 这样可以保证当嵌入的数据量较小时引入到系统的噪声强度也相应减小, 且可将噪声分布到整幅图像中, 使之更接近自然噪声的特性. 由于方差 σ^2 对应着嵌入噪声的幅值, 且容易证明式(3) 是与序列幅值无关的, 因此式(6) 给出的检测算法仍然可行. 但需要注意到较小方差时随机调制后的噪声估计值包含过多的图像本身噪声, 因此在嵌入数据量较小时很难检测到两幅图像中的噪声同步.

为了研究两幅图像的嵌入信息量与估计噪声相关值的关系, 选择 800 幅 256 × 256 的灰度图像进行实验. 随机选取信息容量 $C \in [0, 0.95]$ 进行自适应选择方差的随机调制嵌入, 得到隐秘图像集合. 图 3 给出了集合中任意 500 对图像在 $\Gamma = 0.5$ 的同步分析下的检测结果. 由图 3 知, 当要求容量 (C_1, C_2) 处

于图 3(b) 的区域 I_1 时(SYN $(s^1, s^2) > 0.5$), 检测器能很好地检测出隐写的存在; 而当 (C_1, C_2) 处于检测区域 I_0 时, 检测器则无法检测出隐写的存在. 根据图 3(b), 可得到在 $\Gamma = 0.5$ 的同步分析下, 自适应随机调制方法的最大平均安全容量



(a)　检测结果分布



(b)　检测结果示意

图 3　自适应随机调制的检测结果

设发送方 Alice 和接收方 Bob 以自适应随机调制方法进行了 N 次传输(N 非常大), 在基于两幅图像的同步攻击下, 当且仅当 $C_i = C_{opt}$ 时系统取得其平均最大安全容量 C_{opt}.

证明　不失一般性, 设 1 次 Alice 安全传输的信息量为 C_1, $C_1 - C_{opt} = \Delta_1 > 0$, 由图 2(b) 曲线凸性知, 在第 2, …, N 次通信中, Alice 的安全信息量不能超过 C_2, $C_2 - C_{opt} = \Delta_2 < 0$, 此时系统的最大平均安全容量为

$$C_{1,N} = \frac{C_1 + (N-1)C_2}{N} = \frac{\Delta_1 + (N-1)\Delta_2}{N} + C_{opt}.$$

由于 N 充分大时 $C_{1,N} \approx C_{opt} + \Delta_2 < C_{opt}$, 当 $\Delta_1 = \Delta_2 = 0$ 即 $C_j = C_{opt}$ ($j = 1, \cdots, N$) 时, $C_{1,N}$ 取得其最大值 C_{opt}. 在 $\epsilon = 0.5$ 的噪声同步分析下, 图像的最大平均安全通信容量为 0.42 □

3.2　双噪声随机调制的噪声同步分析

在双噪声 SM 嵌入方法中, 嵌入 -1 或 1 的信息比特就意味着在嵌入点 x_i 加上 n_i^1 或者 n_i^2 的噪声分量, n^1, n^2 分别由 $K_{21} = [\text{seed}_1, \sigma_1]$ 和 $K_{22} = [\text{seed}_2, \sigma_2]$ 产生. 设隐秘图像 s^1 和 s^2 上各选择了 p_1, p_2 的像素用于承载噪声序列, 对 s^1 嵌入点 x_i 上叠加 n_i^1 的概率为 $p_1/2$, 叠加 n_i^2 的概率为 $p_1/2$; 同理, 在 s^2 嵌入点 x_i 上叠加 n_i^1 的概率为 $p_2/2$, 叠加 n_i^2 的概率为 $p_2/2$. 因此 x_i 和 x_i 中的嵌入噪声也具有 $\min(p_1, p_2)/2$ 的相同成分, 当 p_1, p_2 较大时, 根据这部分同步噪声仍然可进行如式(6) 的同步攻击.

针对 512 × 512 的 Lena 和 Jet 灰度图像, 表 1 给出了在不同方差组合下的理论最大容量和不引起 $\Gamma = 0.5$ 的检测器得到检测的安全容量, 最大安全容量是通过调节 $\min(p_1, p_2)$ 以不引起检测器发现得到的.

表 1　不同方差值组合下的最大安全容量

(σ_1^2, σ_2^2)	安全容量	理论容量
(0.1, 0.1)	0.505 0	0.505 0
(0.3, 0.5)	0.605 0	0.605 0
(1.1, 1.5)	0.452 2	0.761 2
(1.3, 1.3)	0.752 5	0.752 5
(1.3, 2)	0.333 9	0.776 8
(1.8, 1.8)	0.201 2	0.789 0
(2, 2)	0.189 0	0.801 2

从表 1 可以看到, 只有在隐写中使用的两个噪声序列方差都比较大时, 同步分析才能准确地发现隐写的存在, 这使得基于双噪声的随机调制方法具有更好的安全性, 对 Lena 和 Jet 的安全容量可达到 0.75. 这是由于当使用两个噪声源时, 同步分析只能发现 $\min(p_1, p_2)/2$ 的同步噪声, 可见噪声的多样性降低了同步攻击的灵敏度.

4　结　　语

基于图像复原、噪声估计和相关性计算, 本文针对使用了固定密钥的随机调制算法中存在的噪声同步性问题, 提出了基于同步分析的隐写检测方法, 并通过相关实验粗略估计了同步分析下随机调制攻击下隐写系统的容量变化. 从分析结果上看, 双噪声调制方法的安全性要高于单随机噪声调制方法, 且随着噪声多样性的增加, 同步分析的成功率相应下降.

传统的隐写分析方法基于单个隐秘对象的统计特征, 根据隐秘图像和自然载体图像之间的统计特性的不同, 实现单个对象是否存在秘密信息的检测. 而本文方法则基于多个隐秘图像的信息, 通过分析图像之间的共有模式, 实现通信双方隐写行为的检测, 这对于跟踪监控可疑对象通信行为的研究具有一定的实用价值. 进一步的实验还表明, 本文方法对文献[7]中的扩频调制隐写也是可行的.

(下转第 579 页)

to Innovative Product Development Using Kino's Model and QFD [J]. *European J of Innovation Management*, 2000, 3(2): 91-99.

[3] 陈以增, 唐加福, 侯荣涛, 等. 基于质量屋的产品设计过程[J]. *计算机集成制造系统*, 2002, 8(10): 757-761.
(Chen Y Z, Tang J F, Hou R T, et al. House of Quality-based Product Development Process [J]. *CIMS*, 2002, 8(10): 757-761.)

[4] Pahl G, Beitz W. *Engineering Design: A Systematic Approach* [M]. London: The Design council, 1998.

[5] 陈以增. *基于质量功能展开的产品开发关键技术及应用研究*[D]. 沈阳: 东北大学, 2003.
(Chen Y Z. *Key Technologies of Product Development Based on QFD with Applications* [D]. Shenyang: Northeastern University, 2003.)

[6] 陈以增, 唐加福, 任朝辉, 等. 基于质量屋的组合方案选择模型[J]. *计算机集成制造系统*, 2003, 9(2): 127-131.
(Chen Y Z, Tang J F, Ren Z H, et al. House of Quality-based Combinatorial Selection Model [J]. *CIMS*, 2003, 9(2): 127-131.)

[7] Finn Wynstra, Arjan van Weele, Mathieu Weggemann. Managing Supplier Involvement in Product Development: Three Critical Issues [J]. *European Management J*, 2001, 19(2): 157-167.

[8] Sobrero, M, Edward B. Strategic Management of Supplier-manufacturer Relations in New Product Development [J]. *Research Policy*, 2002, 31(1): 159-182.

[9] Finn Wynstra, Axelsson B, Weele A. Driving and Enabling Factors for Purchasing Involvement in Product Development [J]. *European J of Purchasing and Supply Management*, 2000, 6(2): 129-141.

[10] Maffinand D, Paul Braiden. Manufacturing and Supplier Roles in Product Development [J]. *Int J of Production Economics*, 2001, 69(2): 205-213.

[11] 赵晓煜, 汪定伟. 选择分销商的模糊综合评判方法[J]. *管理工程学报*, 2002, 16(2): 18-21.
(Zhao X Y, Wang D W. Fuzzy Synthesis Evaluation for Distributor Selection [J]. *J of Management Engineering*, 2002, 16(2): 18-21.)

[12] 杨纶标, 高英仪. *模糊数学原理及应用*[M]. 第3版. 广州: 华南理工大学出版社, 2002.
(Yang L B, Gao Y Y. *Fuzzy Mathematics Principle and Applications* [M]. 3rd ed. Guangzhou: South China University of Technology Press, 2002.)

[13] Hauser J R, Clausing D. The House of Quality [J]. *Harvard Business Reviiew*, 1988, (5-6): 63-73.

[14] 林志航, 车阿大. 质量功能研究现状及进展——兼谈对我国QFD 研究与应用的看法[J]. *机械科学与技术*, 1998, 17(1): 119-121.
(Lin Z H, Che A D. State-of-the-art of QFD: Comments on Research and Application of QFD in China [J]. *Mechanical Science and Technology*, 1998, 17(1): 119-121.)

(上接第575 页)

参考文献(References)

[1] Fridrich J, Goljan M, Du R. Detection of LSB Steganography in Color and Grayscale Images [J]. *IEEE Trans on Multimedia*, 2001, 8(4): 22-28.

[2] Fridrich J, Goljan M, Hogea D. New Methodology for Breaking Steganographic Techniques for JPEGs [A]. *SPIE Proc Electronics Image* [C]. California: SPIE, 2003: 143-155.

[3] Dumitrescu S, Wu X L, Wang Z. Detection of LSB Steganography via Sample Pair Analysis [J]. *IEEE Trans on Signal Processing*, 2003, 51(7): 1995-2006.

[4] Zhang T, Ping X J. A New Approach to Reliable Detection of LSB Steganography in Natural Images [J]. *Signal Processing*, 2003, 83(10): 2085-2093.

[5] Farid H. Detecting Hidden Message Using Higher-order Statistical models [A]. *IEEE Int Conf on Image Processing* [C]. Rocheste: IEEE, 2002: 905-908.

[6] Avcibas I, Memon N, Sankur B. Steganalysis Using Image Quality Metrics [J]. *IEEE Trans on Image Processing*, 2003, 12(2): 221-229.

[7] Marvel L M, Boncelet C G, Retter C T. Spread Spectrum Image Steganography [J]. *IEEE Trans on Image Processing*, 1999, 8(8): 1075-1083.

[8] Fridrich J, Goljan M. Digital Image Steganography Using Stochastic Modulation [A]. *SPIE Proc Electronics Image* [C]. California: SPIE, 2003: 191-202.