文章编号: 1001-0920 (2011) 08-0000-00

基于 D-S 证据理论的融合图像隐写分析

孙子文, 李 慧, 纪志成

(江南大学 通信与控制工程学院，江苏 无锡 214122)

摘 要: 提出一种基于证据权的 D-S 证据理论的图像隐写分析方法. 首先在空域, 离散余弦变换 (DCT) 域和离散小波变换 (DWT) 域分别提取图像特征并各自进行预分类; 然后对各域分类结果进行基本概率分配并进行证据权修正, 利用 D-S 组合规则计算融合概率分配函数, 形成最终的决策级融合分类结果. 针对典型的隐写方法 (如 F5, JPHide, Jstego 和 YASS 算法) 进行检测, 仿真结果显示, 所提出的方法能显著提高单分类器的性能.

关键词: 融合决策； 隐写分析； D-S 证据理论； 证据权

中图分类号: TP391 **文献标识码:** A

Fusion image steganalysis based on Dempster-Shafer evidence theory

SUN Zi-wen, *LI Hui*, *JI Zhi-cheng*

(School of Communication and Control Engineering，Jiangnan University，Wuxi 214122，China. Correspondent：SUN Zi-wen，E-mail：sunziwen@jiangnan.edu.cn)

Abstract: Based on evidence weight and Dempster-Shafer(D-S) evidence theory, an image steganalysis scheme is presented. The image is classified predictively by the characters extracted from spatial, discrete cosine transform(DCT) and discrete wavelet transform(DWT) domain respectively. The basic probability assignments of varies classified results are assigned and modified by evidence weight. Then the fusion probability assignment function is computed by Dempster's combinational rule, and the last decision level fusion classify result is obtained. The detection works are presented to attack typical steganographical schemes such as F5, JPHide, Jstego and YASS. The simulation results show that the presented method can significantly improve the performance of single classifier.

Key words: fusion decision； steganalysis； D-S evidence theory； evidence weight

1 引 言

隐写术通过掩蔽载体中嵌入机密信息进行隐匿通信, 隐写分析则是揭示机密信息的存在并进一步提取出机密信息的技术. 隐写分析算法分为专用隐写分析和通用隐写分析. 通用隐写分析方法大多从空域和变换域 (如离散余弦变换 (DCT) 和离散小波变换 (DWT) 域) 提取特征, 或从单个/多个数据域中提取特征进行隐写分析. 但仅从特征提取角度提高检测性能具有一定的局限性. 典型的 F5, JPHide 和 Jsteg 隐写方法能够抵抗低阶统计分析, 如 Solanki 等人[1-2]提出的抗通用隐写分析的 YASS (yet another steganographic scheme) 算法及其改进算法.

近年来, 人们开始研究应用信息融合技术进行融合隐写分析. Kharrazi 等人[3]对不同隐写分析分类结果进行了决策级最大值融合和均值融合; Andrew[4]采用融合结构特征和最大似然的方法实现了对最不重要比特位 (LSB) 隐写信息容量的有效估计; Rodriguez 等人[5]采用方差加权平均融合和高斯加权平均融合方法实现了决策级融合; 随后, Rodriguez 等人[6]又运用多级分类器和贝叶斯模型平均融合识别 JPEG (联合图像专家小组) 隐写图像嵌入算法; Jing 等人[7]提出的特征选择 (BFS) 特征级融合隐写分析方法融合了 3 种典型高阶统计特征, 实现了对 6 种典型隐写算法的有效检测; 文献 [8] 提出了 DCT 域特征融合隐写分析方法.

本文研究基于不确定性推理 D-S 证据理论的多源信息融合技术以实现融合隐写分析. 首先从空域, DCT 域和 DWT 域提取特征向量; 然后将三域特征向量分别经支持向量机 (SVM) 进行局部决策; 最后运用 D-S 证据理论推理进行全局决策.

收稿日期: 2010-04-24； **修回日期:** 2010-07-04.

基金项目: 国家自然科学基金项目(60774030)； 中央高校基本科研业务费专项资金项目(JUSRP21131).

作者简介: 孙子文(1968−), 女, 副教授, 博士, 从事信息隐藏、模式识别与图像处理等研究； 纪志成(1959−), 男, 教授, 博士生导师, 从事非线性控制、智能控制等研究.

2 带证据权的D-S证据理论

D-S 证据理论是一种不确定推理模型, 被广泛地用于处理互补信息和不确定信息的数据融合算法. 其优势在于能够将大量繁杂的、不同方面的、主观不确定信息, 通过D-S 证据理论信息融合原理有效地转化为确定性的决策结果, 在信息融合技术中往往用来对多个证据组合进行不确定性决策[9].

2.1 基本概念

证据理论用集合表示命题. 对于问题领域的所有可能取值定义 N 个详尽和排他性非空假设的一个非空集合 Θ, 称为样本空间或识别框架. Θ 的所有子集组成的集合记为 2^{Θ}.

定义 1 在识别框架 Θ 上, 假设 A 的基本概率分配函数 (BPA) $m(A)$ 是一个 $2^{\Theta}\to[0,1]$ 的函数, 且满足

$$\begin{cases} m(\varnothing)=0, \\ \displaystyle\sum_{A\subseteq\Theta} m(A)=1, \end{cases} \tag{1}$$

其中 $\varnothing$ 为空集. 使得 $m(A)>0$ 的 A 称为焦元. BPA 的基本作用是对命题进行可信度分配, $m(A)$ 反映了证据对识别框架中命题 A 的支持程度.

定义 2 任何假设 A 的信任函数定义为其所对应的所有子集的基本概率函数之和, 即

$$\mathrm{Bel}(A)=\sum_{B\subseteq A} m(B),\ \forall A\in 2^{\Theta}. \tag{2}$$

信任函数表示命题 A 为真的信任程度, $\mathrm{Bel}(\varnothing)=0$, $\mathrm{Bel}(\Theta)=1$.

定义 3 任何假设 A 的似真函数定义为

$$\mathrm{Pl}(A)=1-\mathrm{Bel}(\bar{A})=\sum_{B\cap A\neq\varnothing} m(B),\ \forall A\in 2^{\Theta}. \tag{3}$$

似真函数表示对 A 为非假的信任程度.

$\mathrm{Bel}(A)$ 和 $\mathrm{Pl}(A)$ 分别表示命题 A 的置信度和似然度, 对于所有 $\mathrm{Pl}(A)$, 均有 $\mathrm{Pl}(A)\geqslant\mathrm{Bel}(A)$. 焦元 A 的信任区间 $\mathrm{El}=[\mathrm{Bel}(A),\mathrm{Pl}(A)]$, 表示对 A 信任的上下限, 用以表示对假设 A 的确认程度. 命题 A 的不确定性可由 $U(A)=\mathrm{Pl}(A)-\mathrm{Bel}(A)$ 描述.

D-S 组合规则通过综合来自不同证据的基本概率分配函数获得融合概率分配函数.

定义 4 设 $m(A_1)$ 和 $m(A_2)$ 是识别框架 Θ 基于不同证据的两个概率分配函数, 按 Dempster 组合规则可合并为

$$m(A)=(m_1\otimes m_2)(A)=\begin{cases} 0,\ A=\varnothing; \\ (1-k)^{-1}\displaystyle\sum_{A_1\cap A_2=A} m_1(A_1)m_2(A_2),\ A\neq\varnothing. \end{cases} \tag{4}$$

设融合系统的识别框架 Θ 包含 N 个完备的互不相容的假设命题, 令其幂集 $2^{\Theta}=\{A_1,A_2,\cdots,A_2^N\}$. 推广同一识别框架 Θ 基于 n 个证据 $e_1,e_2,\cdots,e_n$ 的概率分配函数 $m_1,m_2,\cdots,m_n$ 的 Dempster 组合规则为

$$m(A)=(m_1\otimes m_2\otimes\cdots\otimes m_n)(A)=\begin{cases} 0,\ A=\varnothing; \\ (1-k)^{-1}\displaystyle\sum_{A_1\cap\cdots\cap A_n=A} m_1(A_1)\cdots m_n(A_n),\ A\neq\varnothing. \end{cases} \tag{5}$$

其中归一化常数

$$k=\sum_{A_1\cap\cdots\cap A_n=\varnothing} m_1(A_1)\cdot m_2(A_2)\cdots m_n(A_n),$$

k 表示不同证据源发生冲突的度量. 若 $k=1$, 则认为证据矛盾, 不能组合基本概率分配函数; 若 $k\neq 1$, 则 $m(A)$ 可确定一个基本概率分配函数.

2.2 证 据 权

当 $k\to 1$, 即证据高度冲突时, 利用式 (5) 可能会导致与实际常理相悖的结果. 为解决此问题, 文献 [10] 利用证据权对基本概率分配函数进行了修正.

m_i,m_j 的距离定义为

$$d(m_i,m_j)=\sqrt{\frac{1}{2}(\langle M_i,M_i\rangle+\langle M_j,M_j\rangle-2\langle M_i,M_j\rangle)}, \tag{6}$$

其中

$$\langle M_i,M_j\rangle=\sum_{A_i}\sum_{A_j} m_i(A_i)m_j(A_j)\frac{|A_i\bigcap A_j|}{|A_i\bigcup A_j|}.$$

m_i,m_j 的近似度定义为

$$s(m_1,m_2)=1-d(m_1,m_2). \tag{7}$$

证据 e_i 的基本概率分配函数与系统中其他证据的基本概率分配函数相似程度之和为

$$\alpha(m_i)=\sum_{j=1,j\neq i}^{n} s(m_i,m_j). \tag{8}$$

关键证据 e_f 定义为

$$\alpha(m_f)=\max_{1\leqslant i\leqslant n}\{\alpha(m_i)\}. \tag{9}$$

各证据 e_i 相对于关键证据的证据权定义为

$$\beta_i=\alpha(m_i)/\alpha(m_f). \tag{10}$$

对证据 e_i 的基本概率分配函数修正为

$$m_i'(A)=\beta_i m_i(A),\ \forall A\in 2^{\Theta},\ A\neq\Theta; \tag{11}$$

$$m_i'(\Theta)=\beta_i m_i(\Theta)+(1-\beta_i). \tag{12}$$

式 (11) 使得证据权小的证据的元素 A 所提供的确定性信息减小; 式 (12) 使得证据权小的证据的不确定性元素 Θ 所提供的不确定性信息增加.

3　基于D-S证据理论的融合隐写分析

3.1　证据选取

采用从多个数据域提取特征分别检测分类的结果概率为证据. 选取空域, DCT域和DWT域中一些对隐写嵌入敏感的特征, 由这些特征分类构成检测隐写的证据.

空域特征选取对空域隐写具有较强敏感性的空域三向差分图像灰度共生矩阵[11]. 取差分图像的水平、垂直和对角三向相邻像素前向差分的绝对值捕捉相邻像素的相关性. 差分图像取值范围限制在 $[0,16]$ 内, 取共生矩阵右上三角总共 $153\times 3=459$ 维特征.

DCT域特征选取DCT块内、块间zigzag差分数组一步转移概率矩阵(TPM)[12]. 图像进行 8×8 分块DCT; 生成块内、块间二维zigzag差分数组; 差分数组均嵌位在阈值 $[-5,5]$ 内; 提取块内、块间差分数组一步TPM上三角矩阵共132维特征.

DWT域特征选取测试图像及其预测误差图像的前3阶频域统计矩[13]. 对图像及其预测误差图像分别进行3级Haar小波分解及第1级对角子带的再一级小波分解共17个子带; 计算各子带特征函数的前3阶绝对矩共102个特征. 依据累计贡献率大于等于92%的主成分进行K-L变换以实现特征降维.

3.2　建立识别框架和证据权概率分配函数

建立识别框架为 $\Theta=\{w_{\rm cover},w_{\rm stego}\}$; 幂集元素为 $\{\{w_{\rm cover}\},\{w_{\rm stego}\},\{w_{\rm cover},w_{\rm stego}\}\}$. $w_{\rm cover}$ 和 $w_{\rm stego}$ 分别表示掩体图像类和隐写图像类. 建立合理的基本概率分配函数较为困难, 因此, 本文采用各证据检测概率作为基本概率分配函数. 设似然矩阵为

$$P(w_{\rm sp}|X)=(p(w_{\rm sps}|X),p(w_{\rm spc}|X)),\tag{13}$$

$$P(w_{\rm dc}|X)=(p(w_{\rm dcs}|X),p(w_{\rm dcc}|X)),\tag{14}$$

$$P(w_{\rm dw}|X)=(p(w_{\rm dws}|X),p(w_{\rm dwc}|X)),\tag{15}$$

分别表示测试图像分别经空域, DCT域和DWT域特征检测分类为隐写图像和掩体图像的概率分布. 设 m_1, m_2 和 m_3 分别表示基于空域, DCT域和DWT域证据的基本概率分配函数, 则有

$$\begin{aligned}&m_1(w_{\rm cover})=p(w_{\rm spc}|X),\\&m_1(w_{\rm stego})=p(w_{\rm sps}|X);\end{aligned}\tag{16}$$

$$\begin{aligned}&m_2(w_{\rm cover})=p(w_{\rm dcc}|X),\\&m_2(w_{\rm stego})=p(w_{\rm dcs}|X);\end{aligned}\tag{17}$$

$$\begin{aligned}&m_3(w_{\rm cover})=p(w_{\rm dwc}|X),\\&m_3(w_{\rm stego})=p(w_{\rm dws}|X);\end{aligned}\tag{18}$$

$$m_1(\Theta)=m_2(\Theta)=m_3(\Theta)=0.\tag{19}$$

由式(6)～(12)可推导出带证据权的修正概率分配函数 $m_i'(w_{\rm cover})$, $m_i'(w_{\rm stego})$, $m_i'(\Theta)$, $i=1,2,3$. 再由式(5)推导出三域证据融合概率分配函数 $m(w_{\rm cover})$ 和 $m(w_{\rm stego})$ 分别为

$$\begin{aligned}m(w_{\rm cover})=&(m_1'\otimes m_2'\otimes m_3')(w_{\rm cover})=\\&(1-k)^{-1}\Big(\prod_{1\leqslant i\leqslant 3}m_i'(w_{\rm cover})\Big),\end{aligned}\tag{20}$$

$$\begin{aligned}m(w_{\rm stego})=&(m_1'\otimes m_2'\otimes m_3')(w_{\rm stego})=\\&(1-k)^{-1}\Big(\prod_{1\leqslant i\leqslant 3}m_i'(w_{\rm stego})\Big),\end{aligned}\tag{21}$$

其中

$$\begin{aligned}(1-k)=&\\\prod_{1\leqslant i\leqslant 3}m_i(m_{\rm cover})+&\prod_{1\leqslant i\leqslant 3}m_i(m_{\rm stego})+2\prod_{1\leqslant i\leqslant 3}m_i(\Theta).\end{aligned}$$

3.3　分布式融合

3.3.1　D-S证据理论分布式融合思想

采用D-S组合规则和分布式融合算法实现基于D-S证据理论的多源证据融合隐写分析. 其主要思想是先将各域特征分别经分类器进行局部决策, 并将局部决策结果采用D-S证据理论推理进行全局决策, 即基于所有数据域的特征预分类的结果所获得的可信度分配, 计算总的融合可信度分配, 进而根据一定的准则做出决策. 具体而言, 将各域特征分别输入分类器进行预分类, 并将分类预测结果作为判断测试图像是否为掩体图像或隐写图像的后验概率, 获得各域证据BPA值; 然后进行D-S证据理论推理, 计算组合证据下融合概率分配函数, 从而得到最终的分类结果.

3.3.2　各域证据局部决策

将三域特征分别进行局部决策, 获得各域证据基本概率分配函数值. 空域特征对JPHide和YASS隐写较为敏感, 表现出较好的检测性能; 对Jsteg隐写具有一定的敏感性; 对F5隐写敏感性相对较弱. DCT域特征对F5隐写具有很强的敏感性, 表现出能以较高的概率检测F5隐写; 对JPHide和Jsteg隐写也有较好的敏感性; 但对YASS隐写不敏感. DWT域特征对JPHide比较敏感, 能以较高的概率检测出JPHide隐写; 对Jsteg和YASS隐写均具有一定的敏感性; 对F5隐写则不太敏感.

3.3.3　组合证据全局决策

利用D-S组合规则获得组合证据融合概率分配函数值 $m(w_{\rm cover})$ 和 $m(w_{\rm stego})$, 依据 $m(w_{\rm cover})$ 和 $m(w_{\rm stego})$ 进行全局决策. 全局决策原则为: 目标类别应具有最大的可信度, 不确定性区间长度必须小于某一阈值. 融合隐写分析决策规则为

$$\begin{cases}X\in w_{\rm cover},\ m(w_{\rm cover})>m(w_{\rm stego});\\X\in w_{\rm stego},\ m(w_{\rm cover})<m(w_{\rm stego}).\end{cases}\tag{22}$$

4 仿真结果及分析

4.1 仿真结果

采用Rocha等人[13]提供的JPEG图像和testing数据集, 分类器选择LIBSVM2.86[15].

检测F5, JPHide和JSteg隐写. 选择testing数据集掩体图像及嵌入率为large, medium, small和tiny的F5, JPHide和JSteg隐写图像各100张, 共计1 300张. large, medium, small和tiny表示机密信息分别占有效信道容量的40%以上, 15%～40%, 5%～15%和5%以下. 用60张掩体图像和对应的隐写图像进行训练, 用40张掩体图像和对应的隐写图像进行测试.

检测基本YASS隐写[1]. 掩体图像选择testing数据集净图500张进行质量因子QF_a的JPEG压缩后图像, 候选数据嵌入带选取zigzag排序的前19个低频DCT系数, 按YASS算法进行最大嵌入容量隐写. 参数设置: 主块大小选择10, 12和14, 图像质量因子QF_a和嵌入质量因子QF_h选择50/50和75/50两种方案, 量化索引调制步长为1, 生成共3 000张隐写图像, 用300张掩体图像和对应的隐写图像进行训练, 剩余200张掩体图像和对应的隐写图像进行测试.

所得结果见表1和表2. 表中TPR (true positive rate), TNR (true negative rate)和A(accuracy)分别为正确接受率、正确否定率和正确检测率; L, M, S和T分别表示嵌入率为large, medium, small和tiny.

表 1 检测 F5, JPHide 和 JSteg 隐写结果

隐写算法	嵌入率	空域检测			DCT域检测			DWT域检测			均值融合检测			投票融合检测			本文方法检测		
		TPR	TNR	A	TPR	TNR	A	TPR	TNR	A	TPR	TNR	A	TPR	TNR	A	TPR	TNR	A
F5	L	52.5	50.0	**51.3**	100	92.5	**96.3**	55.0	77.5	**66.3**	97.5	92.5	**95.0**	27.5	97.5	**62.5**	95.0	92.5	**93.8**
	M	65.0	60.0	**62.5**	95.0	92.5	**93.8**	57.5	62.5	**60.0**	92.5	92.5	**92.5**	35.0	100	**67.5**	92.5	92.5	**92.5**
	S	42.5	55.0	**48.8**	97.5	95.0	**96.3**	60.0	57.5	**58.8**	95.0	92.5	**93.8**	27.5	97.5	**62.5**	92.5	92.5	**92.5**
	T	52.5	37.5	**45.0**	97.5	90.0	**93.8**	65.0	57.5	**61.3**	97.5	92.5	**95.0**	32.5	95.0	**63.8**	97.5	92.5	**95.0**
平均检测效果		53.1	50.6	**51.9**	97.5	92.5	**95.0**	59.4	63.8	**61.6**	95.6	92.5	**94.1**	30.6	97.5	**64.1**	94.4	92.5	**93.4**
JPHide	L	92.5	85.0	**88.8**	92.5	80.0	**86.3**	100	90.0	**95.0**	97.5	90.0	**93.8**	87.5	92.5	**90.0**	97.5	90.0	**93.8**
	M	90.0	60.0	**75.0**	72.5	77.5	**75.0**	90.0	82.5	**86.3**	97.5	75.0	**86.3**	55.0	92.5	**73.8**	100	77.5	**88.8**
	S	60.0	77.5	**68.8**	80.0	85.0	**82.5**	87.5	82.5	**85.0**	85.0	80.0	**82.5**	47.5	97.5	**72.5**	82.5	85.0	**83.8**
	T	67.5	75.0	**71.3**	80.0	70.0	**75.0**	60.0	75.0	**67.5**	77.5	75.0	**76.3**	40.0	97.5	**68.8**	80.0	75.0	**77.5**
平均检测效果		77.5	74.4	**75.9**	81.3	78.1	**79.7**	84.4	82.5	**83.4**	89.4	80.0	**84.7**	57.5	95.0	**76.3**	90.0	81.9	**85.9**
Jsteg	L	67.5	75.0	**71.3**	87.5	77.5	**82.5**	77.5	77.5	**77.5**	80.0	80.0	**80.0**	47.5	100	**73.8**	80.0	82.5	**81.3**
	M	75.0	75.0	**75.0**	72.5	75.0	**73.8**	80.0	82.5	**81.3**	80.0	82.5	**81.3**	60.0	95.0	**77.5**	77.5	85.0	**81.3**
	S	70.0	65.0	**67.5**	80.0	72.5	**76.3**	67.5	77.5	**72.5**	77.5	70.0	**73.8**	50.0	87.5	**68.8**	77.5	67.5	**72.5**
	T	75.0	75.0	**75.0**	77.5	75.0	**76.3**	82.5	62.5	**72.5**	85.0	67.5	**76.3**	50.0	87.5	**68.8**	85.0	70.0	**77.5**
平均检测效果		71.9	72.5	**72.2**	79.4	75.0	**77.2**	76.9	75.0	**75.9**	80.6	75.0	**77.8**	51.9	92.5	**72.2**	80.0	76.3	**78.1**

表 2 检测 YASS 隐写结果

嵌入主块大小	QF_h/QF_a	空域检测			DCT域检测			DWT域检测			本文方法检测		
		TPR	TNR	A	TPR	TNR	A	TPR	TNR	A	TPR	TNR	A
10	50/50	91.50	95.00	**93.25**	73.50	72.50	**73.00**	74.50	81.50	**78.00**	95.00	95.50	**95.25**
	75/50	91.00	95.00	**93.00**	33.50	49.50	**41.50**	73.50	76.50	**75.00**	86.50	91.00	**88.75**
12	50/50	91.50	95.00	**93.25**	35.00	42.00	**38.50**	73.50	77.50	**75.50**	89.00	95.00	**92.00**
	75/50	92.00	95.00	**93.50**	32.00	46.00	**39.00**	75.00	77.50	**76.25**	87.00	91.00	**89.00**
14	50/50	91.50	95.00	**93.25**	33.50	49.00	**41.25**	76.50	79.50	**78.00**	88.00	93.50	**90.75**
	75/50	90.50	95.00	**92.75**	33.50	43.50	**38.50**	77.50	76.50	**77.00**	89.50	91.50	**90.50**
平均检测效果		91.33	95.00	**93.17**	40.17	50.42	**45.29**	75.08	78.17	**76.63**	89.17	92.29	**91.04**

4.2 融合效果分析

采用相同的仿真方案进行均值融合和投票融合, 对比仿真结果如表1所示. 简单的投票融合仅根据每个证据的判决, 取多数证据的意见为最终决策, 而不考虑每个证据对结论支持的可信度, 因而检测性能相对较差. 均值融合根据每个证据判决概率的平均值, 取概率平均值大的类为最终决策, 因考虑了每个证据的可信度, 故取得了较好的检测性能. D-S证据理论具有坚实的理论基础, 所提出的D-S融合决策总体检测性能略高于均值融合.

YASS算法由于具有良好的嵌入位置随机性, 典型的隐写分析方法不能对其进行检测[1-2]; 而由表2的仿真结果显示, 本文提出的方法对YASS具有较好的检测效果.

5 结　论

在图像三域各自构造特征, 并根据特征各自预分类产生局部决策; 然后基于信息融合的思想和D-S证据理论, 对三域预分类局部决策进行决策层融合, 形成最终的全局决策. 决策层融合了各域特征分类的结果, 能有效提高分类性能. 仿真结果表明, 相对于单域特征分类, 融合隐写分析算法的检测率得到了提高, 同时误检率有所降低. 对比投票决策和均值决策融合, D-S融合决策具有更高的总体检测性能.

参考文献(References)

[1] Solanki K, Sarkar A, Manjunath B S. YASS: Yet another steganographic scheme that resists blind steganalysis[C]. Lecture Notes in Computer Science. Berlin: Springer, 2007, 4567: 16-31.

[2] Sarkar A, Solanki K, Manjunath B S. Further study on YASS: Steganography based on randomized embedding to resist blind steganalysis[C]. Proc of SPIE-IS&T Electronic Imaging, Security, Forensics, Steganography, and Watermarking of Multimedia Contents X. San Jose: SPIE Press, 2008, 6819-681917: 1-11.

[3] Kharrazi M, Sencar H, Memon N. Improving steganalysis by fusion techniques: A case study with image steganalysis[C]. Proc of SPIE. San Jose: SPIE Press, 2006: 123-137.

[4] Andrew D K. A fusion of maximum likelihood and structural steganalysis[C]. Lecture Notes in Computer Science. Berlin: Springer, 2007, 4567: 204-219.

[5] Benjamin M R, Gilbert L P, Sos S A. Multi-class classification averaging fusion for detecting steganography[C]. Proc of IEEE Int Conf on System of Systems Engineering. Washington DC: IEEE, 2007: 1-5.

[6] Rodriguez B, Peterson G, Bauer K. Fusion of steganalysis systems using Bayesian model averaging[C]. IFIP Int Federation for Information Processing. Boston: Springer, 2008: 345-355.

[7] Dong J, Chen X C, Guo L, et al. Fusion based blind image steganalysis by boosting feature selection[C]. Lecture Notes in Computer Science. Berlin: Springer, 2008, 5041: 87-98.

[8] 孙子文, 纪志成. 基于马尔可夫模型和特征融合的图像隐写分析[J]. 控制与决策, 2009, 24(8): 1039-1242.
(Sun Z W, Ji Z C. Image steganalysis based on Markov model and feature fusion[J]. Control and Decision, 2009, 24(8): 1039-1242.)

[9] 王润生. 信息融合[M]. 北京: 科学出版社, 2007: 4-15.
(Wang R S. Information fusion[M]. Beijing: Science Press, 2007: 4-15.)

[10] 刘海燕, 赵宗贵, 刘熹. D-S证据理论中冲突证据的合成方法[J]. 电子科技大学学报, 2008, 37(5): 701-704.
(Liu H Y, Zhao Z G, Liu X. Combination of conflict evidences in D-S theory[J]. J of University of Electronic Science and Technology of China, 2008, 37(5): 701-704.)

[11] Sun Z W, Hui M M, Guan C. Steganalysis based on co-occurrence matrix of differential image[C]. Proc of IIHMSP 2008. Harbin, 2008: 15-17.

[12] 孙子文, 纪志成. 基于离散余弦变换域的块相关性和马尔可夫模型的图像隐写分析[J]. 信息与控制, 2009, 38(5): 602-607.
(Sun Z W, Ji Z C. Image steganalysis based on block correlation and markov model in DCT domain[J]. Information and Control, 2009, 38(5): 602-607.)

[13] 孙子文, 周治平, 李慧. 基于小波子带特征函数矩和主成分分析的图像隐写分析方法[J]. 信息网络安全, 2009(7): 41-43.
(Sun Z W, Zhou Z P, Li H. An image steganalysis method based on characteristic function moments of wavelet subbands and PCA[J]. Information Net Work Security, 2009(7): 41-43.)

[14] Rocha A, Goldenstein S, Scheirer W, et al. The unseen challenge data sets[C]. IEEE Computer Society Conf on Computer Vision and Pattern Recognition Workshops. Washington DC: IEEE Computer Society, 2008: 1-8.

[15] Chang C C, Lin C J. LIBSVM: A library for Support Vector Machines[EB/OL]. [2008-09-10]. http://www.csie.ntu.edu.tw/cjlin/libsvm/