◎学术探讨◎

# 一种针对 BLOCK-DCT 隐写的隐写分析改进算法

张汗灵,张利平
ZHANG Han-ling,ZHANG Li-ping

湖南大学 计算机与通信学院,长沙 410082
School of Computer and Communication,Hunan University,Changsha 410082,China

**ZHANG Han-ling,ZHANG Li-ping.Improved steganalysis based on BLOCK-DCT steganography.Computer Engineering and Applications,2007,43(14):25-26.**

**Abstract**: BLOCK-DCT based information embedding methods introduce distinctive non-stationarites into the stego-image,which makes the difference distributions between neighboring pixel intensities in one block and across two blocks.While in the cover image these two distributions are indeed remarkably similar.So we use Kolomogrov-smirnov test on these two neighboring pixel populations to test binary hypothesis.In order to improve detective ability,we add absolute value and 8-domain to pairs of neighboring pixel.Theories and experiments both prove that our method is efficiency.

**Key words**: BLOCK-DCT;Kolomogrov-smirnov test;steganalysis

**摘 要**:BLOCK-DCT 隐写算法对平稳性质的原始图像引入了非平稳性,使得隐写图像块内部的相邻像素对与块之间的像素对的分布存在着差异。在未嵌入消息的原始图像中它们的分布是一致的。利用 Kolomogrov-smirnov test(K-s test)去判定图像是否隐藏信息。采用 4 邻域像素对的直接像素差的分布,在 K-s test 中并不怎么理想,两类概率分布之差的上界 $D$ 都比较小。这里通过引入差的绝对值和 8 领域像素对来扩大 2 类像素对分布差异的方法来提高 $D$ 的值,使得一些在以 4 邻域直接像素差分布方法中检测不出的隐写图像在改进的方法中得以检测。理论和实验都证明此方法是有效的。

**关键词**:BLOCK-DCT;Kolomogrov-smirnov test;隐写术分析
**文章编号**:1002-8331(2007)14-0025-02 **文献标识码**:A **中图分类号**:TP301

## 1 引言

隐写术是信息隐藏的一个前沿领域,主要研究如何将实际存在的信息隐藏于正常载体(文字,图像,声音等)中。如果载体是图像就称图像隐写技术,其包括空域隐写(如 LSB)和变化域隐写(如针对 DCT 变换系数的频谱扩展技术)。而隐写术分析的目标是为了检测秘密消息的存在以至破坏或提取隐秘通信。其检测技术一般分为对比检测技术和盲检测技术。其主要差别在于是否有原始图像。

典型的变换域隐写如 BLOCK-DCT 隐写技术[1],是将消息隐藏在 8*8 块的 DCT 系数中。块与块之间消息分布是独立的。Constantine Manikopoulos,Yun-Qing Shi 等提出以水印图像和非水印图像的 BLOCK-DCT 变换系数的差异作为特征向量,然后用神经网络分类图片[2],进而判断图像是否存在隐写消息。其优点是因为存在原始非水印图像,使得检测准确度比较高,采用特征向量能够反映很多图像的平均统计特性,但这平均统计特性有时未必符合某个具体的图像个体统计特性。并且算法复杂度高。Ying wang 提出,由于隐写后的图像引入了非平稳性,使得 8*8 块内部的相邻像素对与块块之间的像素对的分布存在不同。而未隐写的图像它们的分布却是一致的[3]。然后利用 K-s 测试给定的图片中 2 类分布是否存在不同,以此来判断图像是否隐藏消息。这给了一个很好的盲检测想法,就是从图像内部 2 类特征的不同来区分图像是否隐写。这种方法不需要原始图像,只根据个体图像统计特性来分析。为了扩大 Ying wang 算法中提出的 2 类分布不同,在其基础上引入了差的绝对值和 8 领域的像素对差。使得 2 类分布假说在 K-s test 中能够更加容易区分,提高了测试的能力。

## 2 改进算法

### 2.1 像素对的选取

消息嵌入的 BLOCK-DCT 模式见参考文献[3],选取 2 组像素,1 组是在块的内部,1 组是在块与块的边界。内部组像素的选取尽可能的反应内部性质,所以选择在内部中间。Ying wang 选择了 4 领域像素对(图 1 方框所示),在其基础上增加了 2 对 8 邻域(图 1 中线条表示)。选择的原因是,嵌入消息后,2 组像素对的分布不同主要是由于隐写图像改变了像素对的相关性。而如果更精确的分析其分布,势必要分析其 8-邻域相关性的影响。

### 2.2 不同像素对的统计差异

首先假设隐写图像是零均值、相关函数 $r_u(k,l)=E[U_{m,n},U_{m-k,n-l}]$ 的 2-D 稳态过程。其灰度值 $U(m,n)$,$m=1,\cdots,M$,$n=1$,

基金项目:国家自然科学基金(the National Natural Science Foundation of China under Grant No.60373062,No.60573045);湖南大学重点基金资助。
作者简介:张汗灵(1968-),男,副教授;张利平(1980-),男,硕士。

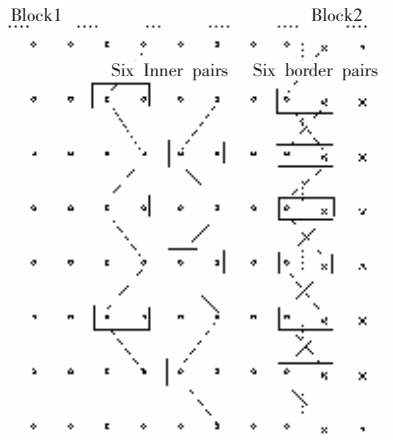


图 1 像素对的选取

…,$N$。

**定义**:

对于 cover image

$$d_{mn}=|U_{m,n}-U_{m,n+1}|+|U_{m,n}-U_{m-1,n+1}|+|U_{m,n}-U_{m+1,n+1}| \tag{1}$$

对于 stego image

$$d'_{mn}=|U'_{m,n}-U'_{m,n+1}|+|U'_{m,n}-U'_{m-1,n+1}|+|U'_{m,n}-U'_{m+1,n+1}| \tag{2}$$

设 $d_0(m,n)$为从块内部像素对按式(1)求得的像素关系。$d_0'(m,n)$为从块内部像素对按定义(2)求得的像素关系。

$d_1(m,n)$为从块块边界对按式(1)求得的像素关系。$d_1'(m,n)$为从块块边界对按式(2)求得的像素关系。

从定义可以看出 $d'_{mn}$ 和 $d_{mn}$ 的分布是 3 项分布的叠加:一项 4 领域分布$|U_{m,n}-U_{m,n+1}|$两项 8 领域分布$|U_{m,n}-U_{m-1,n+1}|$和$|U_{m,n}-U_{m+1,n+1}|$。

(1)cover image 分析

Ying wang 定义 $d_{m,n}=U_{m,n}-U_{m,n-1}$,并证明指出 $d_0(m,n)$与 $d_1(m,n)$服从$\sim N(0,2[\sigma_u^2-r_u(1)])$同一正态分布[1]。那么仅由$|U_{m,n}-U_{m,n-1}|$定义的 $d_0(m,n)$与 $d_1(m,n)$也服从同一分布。同理,分别仅由 8 领域$|U_{m,n}-U_{m-1,n+1}|$和$|U_{m,n}-U_{m+1,n+1}|$定义的 $d_0(m,n)$,$d_1(m,n)$,也服从同一分布。

那么,如果用式(1)来定义,并以此求得的 $d_0(m,n)$与 $d_1(m,n)$肯定也服从同一分布。

(2)steg image 分析

嵌入消息 $Z(m,n)$后,在块的内部像素对会引入相关性,而在块与块之间像素对 $Z$ 的相关性为零。虽然取式(1)的 $d_{m,n}$ 因引入绝对值,其分布不属于正态分布,但同样可以分析其方差来分析分布的不同。忽略 4 领域像素对与 8 领域像素对之间的相关性,求得方差为:

$$\sigma^2_{d'_0}(m,n)=A-2\left[r_z\begin{pmatrix}m & m\\ n & n+1\end{pmatrix}+r_z\begin{pmatrix}m & m-1\\ n & n+1\end{pmatrix}+r_z\begin{pmatrix}m & m+1\\ n & n+1\end{pmatrix}\right] \tag{3}$$

$$\sigma^2_{d'_1}(m,n)=A$$

$$\begin{aligned}A=&3\sigma_u^2(m,n)+\sigma_u^2(m,n+1)+\sigma_u^2(m-1,n+1)+\\ &\sigma_u^2(m+1,n+1)+3\sigma_z^2(m,n)+\sigma_z^2(m,n+1)+\\ &\sigma_z^2(m-1,n+1)+\sigma_z^2(m+1,n+1)+E(d_0')\\ &-2\left[r_u\begin{pmatrix}m & m\\ n & n+1\end{pmatrix}+r_u\begin{pmatrix}m & m-1\\ n & n+1\end{pmatrix}+r_u\begin{pmatrix}m & m+1\\ n & n+1\end{pmatrix}\right]\end{aligned} \tag{4}$$

比较上面式(3),(4)知,$\sigma^2_{d'_0}(m,n)$和 $\sigma^2_{d'_1}(m,n)$是属于不同的分布,主要的不同在于:$2\left[r_z\begin{pmatrix}m & m\\ n & n+1\end{pmatrix}+r_z\begin{pmatrix}m & m-1\\ n & n+1\end{pmatrix}+r_z\begin{pmatrix}m & m+1\\ n & n+1\end{pmatrix}\right]$项。

这是由于嵌入的消息在块与块之间是独立的,所以当计算块块像素对的分布时这一项就消失了。而仅用 4 领域像素对,得出的不同项为 $2r_z\begin{pmatrix}m & m\\ n & n+1\end{pmatrix}$[3]。可知增加 8 领域扩大了分布的不同。

### 2.3 利用 Kolomogrov-smirnov test 区分 2 类分布假说

具体的假说测试可详见文献[3],根据 K-s 测试理论[4],$D_{M,N}>D_{M,N,\alpha}$ 的分布与 $S_0(x)$,$S_1(x)$的分布无关。所以在假设 $H_0$:$F_0=F_1$(即:未隐写的 cover image)下,$\sqrt{\frac{MN}{M+N}}D_{M,N}$ 的分布仍然满足以下关系:

$$\lim_{M,N\to\infty}P_0\left(\sqrt{\frac{MN}{M+N}}D_{M,N}\leqslant d\right)=1-2\sum_{k=1}^{\infty}(-1)^{k-1}e^{-2k^2d^2}$$

并在设定误差概率 $\alpha$ 下,可以通过查表来求出 $d$,然后求出域值 $D_{M,N,\alpha}$。

引入绝对值并没有改变未嵌入消息的图像 2 类分别相同的特性,但却可以扩大隐写后图像 2 类分别不同的差异,使得对称的差异得到叠加。

增加绝对值和 8 领域虽然改变了像素对的分布,可并未影响在 $H_0$ 假设下、在同一误差水平下,域值 $D_{M,N,\alpha}$ 的大小。但是却提高了在 $H_1$:$F_0\neq F_1$(即:steg image)假说下,通过隐写图像像素对采样求得的 $D_{M,N}=\sup_x|S_0(x)-S_1(x)|$值。以此提高了检测精度。

## 3 实验结果和总结

表 1 是 2 种方法的比较。

从图 2 明显的看出,在相同的误警概率下,改进的算法明显提高了通过像素对采样求得的 $D_{M,N}$,当 $D_{M,N}>D_{M,N,\alpha}$,认为图像

表 1 Ying wang 算法 VS 改进算法

| $d_e$ | $D_{M,N}$ | | | |
|---|---|---|---|---|
| | Ying wang 算法 | | 改进算法 | |
| | Lena | Baboon | Lena | Baboon |
| 0.025 | 0.020 8 | | 0.032 9 | |
| 0.050 | 0.024 1 | 0.008 67 | 0.041 7 | 0.007 67 |
| 0.075 | 0.028 7 | | 0.053 7 | |
| 0.100 | 0.033 9 | 0.011 1 | 0.062 6 | 0.013 80 |
| 0.150 | | 0.014 6 | | 0.022 80 |
| 0.200 | | 0.017 4 | | 0.030 90 |
| 0.250 | | 0.019 9 | | 0.036 30 |

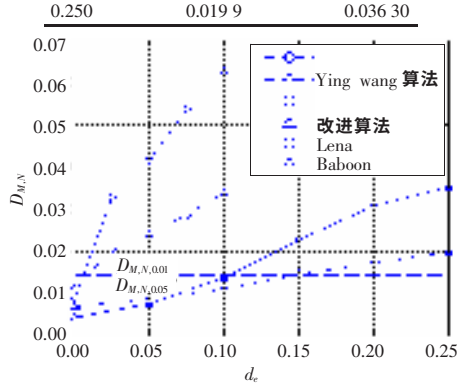


图 2 Ying wang 算法 VS 改进算法

(下转 63 页)