基于统计数学的伪随机序列与图像正交性分析

房 波 陈惠芳 胡炯炯
(浙江大学信息与电子工程学系,杭州 310027)

摘 要 在数字图像水印、图像加密等领域,经常需要一个与图像正交的伪随机序列。为了获得具有较好正交效果的伪随机序列,基于统计数学的方法,推导出了一个自然图像与伪随机序列两者互相关的二阶数字特征在空域和频域的表达式。结果显示,具有高通型频谱特征的伪随机序列,例如游程受限(run-length limited, RLL)序列,在与图像的正交性方面,比目前广泛使用的白噪声序列性能更优。统计实验也证实了上述结论和该数学模型的有效性。另外,为了快速生成 2 维 RLL 序列,还给出了一种简便易行的 2 维 RLL 序列生成算法。

关键词 数字水印 平稳随机过程 正交性 m 序列 RLL 序列
中图法分类号: TP309 **文献标识码**: A **文章编号**: 1006-8961(2005)03-0365-07

Statistical Analysis of the Orthogonality Between Images and Pseudo-random Sequences

FANG Bo, CHEN Hui-fang, HU Jiong-jiong
(*Department of Information Science & Electronic Engineering, Zhejiang University, Hangzhou* 310027)

Abstract In digital image watermarking and image encryption, researchers often require a pseudo-random sequence which is statistically orthogonal to an image. The white noise sequences, such as m-sequence, are often used in these situations. But our study shows they are not optimum on orthogonal property. To get a better orthogonality, we studied the cross-correlation of unartificial images and pseudo-random sequences by means of statistical mathematics method. The second-order expectation of the cross-correlation value was determined in both space and frequency domains. The expression suggests that sequences which are high-pass in frequency domain, like Run-Length Limited (RLL) sequences, have better orthogonal character with unartificial images than white noise sequences which are widely used at present. The conclusion and the validity of our mathematical model were also proved by the result of statistical experiments. In order to generate 2D-RLL sequences rapidly, we developed a simple and convenient algorithm. The experiments that confirmed 2D-RLL sequences have better orthogonality with natural images than m-sequences.

Keywords digital watermarking, stationary stochastic process, orthogonality, m-sequence, RLL-sequence

1 引 言

随着 Internet 的迅速发展,用于保护数字版权的水印技术得到了人们越来越多的重视。Trikel 等人首先注意到了扩频技术可以应用于数字水印[1]。由于该技术抗干扰能力强,因此扩频水印逐渐成为研究的热点。

1996 年,Hartung 等人提出了如下一种空域扩频水印方案[2,3]:

$$\hat{g}_{i,k} = g_{i,k} + \alpha_k b_k l_{i,k}$$

其中,$g_{i,k}$是原始第 k 块图像中第 i 个像素的灰度值,$\hat{g}_{i,k}$是嵌入水印后的像素灰度值,α_k 是嵌入强度系数,b_k 是水印比特,取值{1, -1},$l_{i,k}$是第 k 个扩频序列中第 i 个元素的值。

水印提取时,对第 k 块图像和第 k 个扩频序列按下式做相关运算:

$$c_k = \sum_i \hat{g}_{i,k} l_{i,k} = \sum_i g_{i,k} l_{i,k} + \alpha_k b_k \sum_i l_{i,k}^2$$

如果图像块和扩频序列正交,则 $\sum_i g_{i,k} l_{i,k} = 0$;当扩频序列是映射到{1, -1}的双极性序列时, $\sum_i l_{i,k}^2$ 为

收稿日期:2004-02-02;改回日期:2004-07-26

第一作者简介:房波(1979 ~),男,2002 年毕业于浙江大学信息与电子工程学系信息工程专业,现为浙江大学信息与电子工程系硕士研究生。主要研究领域为图像处理,多媒体通信。E-mail:fbcome@yahoo.com.cn

常数,此时由 c_k 的正负即可判断出嵌入的比特 b_k。

要生成严格与某幅特定图像正交的扩频序列,虽可以采用特征值分解的方法[4],但由于此方法计算量大,并且水印提取时,尚必须拥有原始图像,因此不符合水印盲检测的要求。实际常用的方法是采用一个和图像无关的伪随机序列作为扩频码。文献[5]建议采用末端补 0 的 m 序列或者用高阶 m 序列的片段作为扩频码。文献[6]采用标准 10 阶 m 序列实现了一个扩频水印方案。另外,在图像处理的其他领域,例如图像加密,也经常需要一个和图像正交的伪随机序列。

在以往的研究中,研究者们普遍把白噪声序列(例如 m 序列、混沌序列[7]等)用作扩频码。本文采用统计数学的方法,首先推导了图像与伪随机序列互相关的二阶数字特征,并由此指出,在与图像的正交性上,高通型序列比白噪声序列更优。

2 统计数学分析

2.1 数学模型

为了简化分析,本文仅考虑灰度图像,且灰度值非负。

一幅数字灰度图像 $\boldsymbol{g}$ 可以被看作是离散随机场 $\boldsymbol{G}$ 的一个实例。进一步可以认为,这个随机场是广义平稳的,并且当像场上各点之间的相关性比例于它们几何上的分离程度时,像场常可模拟为一阶马尔可夫过程[8]。

设 G_i 为图像场 $\boldsymbol{G}$ 中位置为 i 的随机变量(i 为离散二元矢量);$\boldsymbol{L}$ 是伪随机序列,被用作扩频码,其中位置为 i 的随机变量被记做 L_i(由于多数伪随机序列都是 1 维序列,例如 m 序列,因此在与图像做相关运算时,通常要将 1 维序列一行一行地"折叠"成 2 维形式[9],或者等价地将图像用"光栅扫描"(raster-scan)成 1 维序列,本文默认情况下是将序列折叠成 2 维形式),且图像场 $\boldsymbol{G}$ 和 $\boldsymbol{L}$ 彼此独立。上述随机变量的某个实例用相应小写字母标记。定义伪随机序列 $\boldsymbol{L}$ 与图像场 $\boldsymbol{G}$ 的互相关系数为

$$\gamma_{cor} \triangleq \sum_i L_i G_i$$

显然它也是随机变量。当 $\gamma_{cor}=0$ 时,则图像 $\boldsymbol{g}$ 和序列 $\boldsymbol{l}$ 正交。实际应用中,只需互相关系数的绝对值小于某个 δ 即可。

2.2 互相关系数 γ_{cor} 的均值

互相关系数的数学期望为

$$E[\gamma_{cor}] = E[\sum_i L_i G_i] = \sum_i E[L_i] \cdot E[G_i]$$

如果图像平稳,即 $E[G_i]$ 为常数,则只需 $E[\sum_i L_i]=0$,就有 $E[\gamma_{cor}]=0$。若图像不平稳,则当序列是平稳的,且均值为 0,即 $E[L_i]=0$ 时,有 $E[\gamma_{cor}]=0$。由于对于大多数自然图像和伪随机序列来说,这两个条件是很容易满足的,因此,当仅考虑一阶数字特征时,绝大多数伪随机序列都能很好地和图像正交,例如用插 0 的方法将周期补齐为 2^n 的 m 序列[9],当将其映射到{-1,1}后,它严格满足 $\sum_i l_i = 0$,并且不同 i 的 L_i 近似两两独立,具有很好的自相关特性。这也是在以往的研究中,人们通常把 m 序列作为扩频序列的原因[1]。

2.3 互相关系数 γ_{cor} 的二阶数字特征

然而,本文在实际应用中发现,仅考虑均值是不够的,还必须考虑互相关系数的以下二阶数字特征:方差和二阶矩。下面以实验 1 来说明这一点。

实验 1 试验图像是 512×512 的 256 级灰度 Lena 图,其灰度值线性映射为[0,1]之间的实数,实验时,首先将原图分为 32×32 大小的图像块,每块图像被视为同分布随机图像场的一个实例;然后采用 10 阶 m 序列作为扩频序列,用插 0 的方法补齐为 2^{10} 点的长度,并映射成{-1,1}的双极性信号。而对每个图像块,则先通过随机产生种子来生成相应 m 序列,然后和图像做相关运算得到 γ_{cor}。表 1 显示了每次实验互相关系数的样本均值 $\bar{\gamma}_{cor}$,样本方差 S^2_{cor},样本二阶矩 A^2_{cor} 及其方根 A_{cor}。

表 1 Lena 图与 m 序列的互相关系数的统计量

Tab. 1 Cross-correlation coefficient of Lena image and m-sequence

实验序号	$\bar{\gamma}_{cor}$	S^2_{cor}	A^2_{cor}	A_{cor}
1	0.0366	12.5	12.4	3.53
2	-0.00699	13.2	13.1	3.62
3	0.0507	13.6	13.6	3.68
4	0.0939	11.2	11.1	3.34
5	-0.0705	12.3	12.2	3.49

从表 1 可以看出,相对于图像灰度值和扩频序列能量,互相关系数的均值很小,其绝对值基本不会超过 0.1,可以说完全满足要求了,但样本方差和二阶矩却大得多。由于当像素之间的相关系数幅值小于 1 时,中心极限定理仍可以适用[10],因此可以假定互相关系数符合 0 均值正态分布。若以标准差为 3.6(方差为 13)计算,就意味着:平均有 32% 的互

相关系数值处于[-3.6,3.6]之外。这样相应地,在设计水印时,即使没有噪声,嵌入强度也不能小于 $3.6/2^{10}=0.0035$,才能保证大约 68% 的比特能被正确地提取出来,此时由水印嵌入所造成的图像峰值信噪比是 49dB,图像质量还可接受,但水印提取率太低,这显然不能令人满意。

因此,有必要从理论上研究互相关系数的二阶数字特征。由于当互相关系数均值为零时,方差和二阶矩相等,因此以下仅研究二阶矩。

γ_{cor}的二阶距:

$$\begin{aligned}\mathrm{E}[\gamma_{cor}^2] &= \mathrm{E}[(\sum_i L_i G_i)(\sum_j L_j G_j)] \\ &= \mathrm{E}[\sum_{i,j} L_i L_j G_i G_j] \\ &= \sum_{i,j} \mathrm{E}[L_i L_j]\cdot \mathrm{E}[G_i G_j]\end{aligned}$$

假设图像平稳,并设伪随机序列也具有平稳性,则

$$\mathrm{E}[G_i G_j] \triangleq R_{img}(i-j)$$

$$\mathrm{E}[L_i L_j] \triangleq R_{seq}(i-j)$$

$$\mathrm{E}[\gamma_{cor}^2] = \sum_{i,j} R_{img}(i-j) R_{seq}(i-j)$$

记 $q \triangleq i-j$,D 为 i,j 的值域,$\hat{D}$ 为 q 的值域,$H(q) \triangleq \{(i,j)$ 的个数 $|i-j=q$,且 $i,j \in D, q \in \hat{D}\}$。

若将 $\mathrm{E}[\gamma_{cor}^2]$改写为对 q 求和,则有

$$\mathrm{E}[\gamma_{cor}^2] = \sum_{q \in \hat{D}} H(q) R_{img}(q) R_{seq}(q) \qquad (1)$$

根据式(1)可知,互相关系数的二阶矩是图像场的自相关函数和扩频序列的自相关函数乘积的加权和。考察式(1)中的 3 个因子可以发现:

(1) $H(q)$是一个关于$\|q\|$($\|\cdot\|$表示取模)的严格单调减函数,且大于 0。当 q 为 2 维矢量时,则 $H(q)$的函数图形是类金字塔形,当 q 为标量时(即图像被扫描成 1 维序列再和伪随机序列做相关),则$H(q)$的函数图形是三角形。$H(0)$等于图像场中 0 像素的个数。

(2) 对于一般的自然图像,文献[8]指出,可以将其模拟成 2 维马尔可夫过程,它的自协方差函数按照$\|q\|$呈指数下降;对于平稳图像,由于自协方差函数和自相关函数仅相差图像均值的平方这个常数项,因此,$R_{img}(q)$也是严格单调减函数,并且 $R_{img}(q) \geqslant 0$,$R_{img}(0)$是图像的二阶矩。

(3) 对于常用扩频序列,例如补齐周期为 2^n 的全周期 m 序列,若将其映射到{ -1,1},则它的自相关函数并不是减函数,但当 q 不为 0 时,则 $R_{seq}(q)$的“起伏”远小于 $R_{seq}(0)=2^n$。

基于以上 3 点,可以得出以下结论:互相关系数的方差/二阶矩主要取决于图像场和扩频序列各自的自相关函数 $R(q)$中$\|q\|$较小的那些项。对于映射到{ -1,1}的伪随机序列,$R_{seq}(0) \equiv 2^l$(l 为序列中元素个数)是一个不依赖于扩频序列具体性质的常量,其表示扩频序列的能量/功率,由于 $H(q)$、$R_{img}(q)$均非负,因此应该选择那些当$\|q\|$较小时,$R_{seq}(q)$很小的伪随机序列来作为扩频码,才能取得较好的正交效果。

2.4　频域分析

在式(1)中,记 $t(q)=H(q)R_{img}(q)$;$t(q)$的实质是对 $R_{img}(q)$加了三角窗 $H(q)$,在计算形式上,其是有限大图像场 G 零延拓后的线性相关函数。

对 $t(q)$和 $R_{seq}(q)$分别做 2D-DFT 变换,即可得 $T(p)$和 $S(p)$,$T(p)$是 $H(q)$的频谱和图像功率谱的卷积,而 $S(p)$则是扩频序列的功率谱。

当 q 为 2 维矢量,即扩频序列被折叠成 2 维形式后再和图像作相关运算时,有

$$\mathrm{E}[\gamma_{cor}^2] = \frac{1}{(2M-1)(2N-1)} \sum_p \|T(p)\| \cdot \|S(p)\| \qquad (2)$$

成立。(图像分块大小为 $M \times N$,上式证明见附录)

若 q 为标量,则上述结论仍成立。

式(2)说明,$\mathrm{E}[\gamma_{cor}^2]$与 $t(q)$和 $R_{seq}(q)$的频谱幅值的互相关系数成正比。对于自然灰度图像,由于 $T(p)$一般为低通型,因此要达到较小的$\mathrm{E}[\gamma_{cor}^2]$,则扩频序列的功率谱 $S(p)$在低频段必须较小。考虑到序列功率谱在整个频段的和正比于 $R_{seq}(0)$,且是个定值,可以得出如下结论:应该选择那些功率谱在高频处有较强分量的伪随机序列作为扩频序列,用于和图像作相关运算。

事实上,从空间域得出的结论和从频域得出的结论是等价的,$R_{seq}(0)$是个定值,而且要求紧邻它的 $R_{seq}(q)$较小,这就意味着扩频序列必然有较强的高频分量。

然而 m 序列等多数伪随机序列通常都被设计成白噪声序列,由于其变量之间近似独立,且它们的频谱在整个频带范围内都是平坦的,因此在二阶数字特征上,这些序列和自然图像并不会有很好的正交性。

2.5　互相关系数 γ_{cor}的条件二阶数字特征

为了方便实际应用,很多时候,由于对于不同的图像块会采用同一个扩频码,因此,有必要研究在 L

序列确定时,互相关系数的各项条件数字特征。

仍假设图像和序列平稳,记 $E[G_i]=\mu$,则互相关系数的条件均值为

$$E[\gamma_{cor}\mid L]=E[\sum_i l_iG_i]=\sum_i (l_iE[G_i])$$

$$=\mu(\sum_i l_i)$$

当 $\sum_i l_i=0$ 时,$E[\gamma_{cor}\mid L]=0$

互相关系数的条件二阶矩为

$$E[\gamma_{cor}^2\mid L]=E[(\sum_i l_iG_i)^2]=E[\sum_i\sum_j l_il_jG_iG_j]$$

$$=\sum_{i,j} l_il_jE[G_iG_j]=\sum_{i,j} l_il_jR_{img}(i-j)$$

$$=\sum_{q\in\hat{D}} R_{img}(q)\sum_{\substack{i\in D\\ i-q\in D}} l_il_{i-q}$$

定义 $r_{seq}(q)\triangleq\frac{1}{H(q)}\sum_{\substack{i\in D\\ i-q\in D}} l_il_{i-q}$,则

$$E[\gamma_{cor}^2\mid L]=\sum_{q\in\hat{D}} H(q)R_{img}(q)r_{seq}(q)\quad(3)$$

互相关系数的条件方差为

$$D[\gamma_{cor}\mid L]=D[\sum_i l_iG_i]=\sum_{i,j}\mathrm{cov}[l_i\Phi_i,l_jG_j]$$

$$=\sum_{i,j} l_il_j\mathrm{cov}[G_iG_j]\triangleq\sum_{i,j} l_il_jC_{img}(i-j)$$

$$=\sum_{q\in\hat{D}} C_{img}(q)\sum_{\substack{i\in D\\ i-q\in D}} l_il_{i-q}$$

$$=\sum_{q\in\hat{D}} H(q)C_{img}(q)r_{seq}(q)$$

上式中,$C_{img}(q)$ 是平稳图像场的自协方差函数,($\mathrm{cov}[\cdot]$ 是求随机变量的协方差)。当 $\|q\|\to\infty$ 时,$C_{img}(q)\to 0$。

当 $E[\gamma_{cor}\mid L]=0$ 时,$E[\gamma_{cor}^2\mid L]=D[\gamma_{cor}\mid L]$。此时,由条件方差的表达式更容易看出,互相关系数的条件方差(或条件二阶矩)取决于参量平均 $r_{seq}(q)$ 中 $\|q\|$ 较小的那些项。

若序列 L 除平稳性外,还满足各态历经的要求,则参量平均可以代替集平均,且参量平均 $r_{seq}(q)$ 是 $R_{seq}(q)$ 的无偏估计[11],即 $r_{seq}(q)\approx R_{seq}(q)$。

由此可以发现,当 $\|q\|$ 变小时,由于参与平均的项数 $H(q)$ 变大,因此 $r_{seq}(q)$ 对 $R_{seq}(q)$ 的近似将会相当精确,而 $\|q\|$ 相对较大的项,则由于其参与平均的项较少,因此估计不准确的可能性比较大,但由于在 $E[\gamma_{cor}^2]$ 和 $E[\gamma_{cor}^2\mid L]$ 中,起主要作用的都是 $\|q\|$ 较小的那些项,因此这种估计偏差的影响并不大。

这样,当图像和扩频序列均平稳,并且序列满足各态历经要求时,比较式(1)和式(3),则有

$$E[\gamma_{cor}^2\mid L]\approx E[\gamma_{cor}^2]$$

由此可见,在一定条件下,对于不同的图像,若使用同一个扩频码,则其性能和使用不同的扩频码的方法是相当的。

事实上,即使 $E[\gamma_{cor}^2\mid L]$ 和 $E[\gamma_{cor}^2]$ 不等,在数学上也有

$$E\{E[\gamma_{cor}^2\mid L]\}=E[\gamma_{cor}^2];$$

并且当 $E[\gamma_{cor}\mid L]=0$ 时,有

$$D[\gamma_{cor}]=E\{D[\gamma_{cor}\mid L]\}+D\{E[\gamma_{cor}\mid L]\}$$

$$=E\{D[\gamma_{cor}\mid L]\}$$

成立。

统计实验 2 和实验 3 的结果也证实了本文的观点。实验 2 和实验 3 均选择 512×512 灰度图,分块大小为 32×32 的 10 阶 m 序列来进行实验。实验 2 中,每次实验各个图像块采用不同种子的 m 序列,实验 3 中,每次实验各个图像块采用相同的 m 序列。两种实验都重复 200 组,但把实验 2 的 200 组结果合并为 1 组样本,再计算样本二阶矩和方差;而把实验 3 的每组结果都视为 1 组样本,再计算出样本统计量的组平均和组标准差,然后和实验 2 的结果进行比较。比较结果见表 2。

表 2 使用不同 m 序列和相同 m 序列的比较

Tab. 2 Comparison between diverse m-sequence and unique m-sequence

图像	$\bar{\gamma}_{cor}(\times10^{-2})$	S_{cor}^2	A_{cor}^2	$\eta(S_{cor})$ (%)	$\eta(A_{cor})$ (%)
Lena	1.15/-1.08	12.4/12.6	12.4/12.6	18	18
Barbara	2.36/-2.39	18.6/18.4	18.6/18.5	17	17
Boats	-2.37/3.23	14.5/14.1	14.5/14.1	17	17
Bridge	1.03/1.95	18.7/18.4	18.7/18.6	13	14

表 2 中,互相关系数的样本均值、样本方差、样本二阶矩 3 项中,"/"前的数据是实验 2 的样本统计量,"/"后的是实验 3 的每组样本统计量的组平均值,表中变异系数 $\eta(S_{cor})$、$\eta(A_{cor})$ 是实验 3 中样本的标准差和样本二阶矩方根的组标准差与相应组均值的比值。

由表 2 可以看出,对于二阶统计量 S_{cor}^2、A_{cor}^2,使用不同 m 序列和使用相同 m 序列的效果在统计意义上非常接近,而对于互相关系数的一阶统计量——样本均值,两种方法有较大的差距,但由于互相关系数的均值远小于二阶统计量的方根,因此在设计水印嵌入强度时,它不起主要作用。同时,观察实

验 3 的变异系数 η 可以发现,在使用固定序列扩频的方案中,具体挑选哪一个序列差别并不大,其所造成的平均偏差度都在 20% 以下。实验结果表明,绝大多数的 m 序列在二阶统计量上都可以和平均值很接近,即具有稳定性,这也正是由于 m 序列具有一定的各态历经性所造成的。

3　游程受限的扩频序列

由式(2)可知,由于要获得好的正交性,就要使用高通型的扩频码,同时,该码又必须是伪随机产生的,因此,可以考虑通过某种调制方式来将原本具有白噪声功率谱的伪随机序列,调制成高通型序列。

3.1　1 维 RLL 扩频序列

由于 1 维序列的频谱理论较为成熟,因此下面先研究 1 维的情况。这时,需把图像由 2 维"扫描"成 1 维。本文采用了 Hilbert-Peano 扫描[12]方法,这是一种分形扫描方法。相比光栅扫描,由于 Hilbert-Peano 扫描线十分不规则,可以形成更平滑的自相关函数,因此可抑制扫描引入的高频分量。

在数字通信中,经常要把信源序列变换成与信道频谱限制相匹配的序列,称为数据转换编码(data transform code,DTC)。对于二元序列,常用的方法是将信源序列转换成(d,k)序列,再经非归零反转,编码成游程受限(run-length limited,RLL)码[13]。由(d,k)序列导出的 RLL 码中连号的长度至少为 $d+1$,至多为 $k+1$。根据计算可以发现,(d,k)约束的主要作用就是重新分配功率谱。由于小的 k 约束是通过减少平均游程长度来将功率分配到高频端,而大的 d 约束则正好相反[14],因此,本文选择游程长度至少为 1,至多为 2 的 RLL 码作为扩频码。

与通常的做法不同,本文采用了直接将 m 序列映射成 RLL 码的方法:将 0 映射成[-1, +1],将 1 映射成[+1, -1];而不经过(d,k)码的转换。因为这样更简单,并且可以保证编码之后必有 $\sum_i l_i = 0$,其付出的代价是编码效率只有 0.5,不可能达到编码效率的理论极限 0.69[13]。

表 3 是采用 m 序列和 1 维 RLL 序列作扩频码时,两者互相关系数样本二阶矩的对比。实验时,图像用 Hilbert-Peano 方法扫描成 1 维序列。在一次实验中,对各个分块图像使用相同的扩频码,各进行 200 次实验。图像大小 512 × 512,分块大小32 × 32,用来映射成 RLL 码的 m 序列为 9 阶。

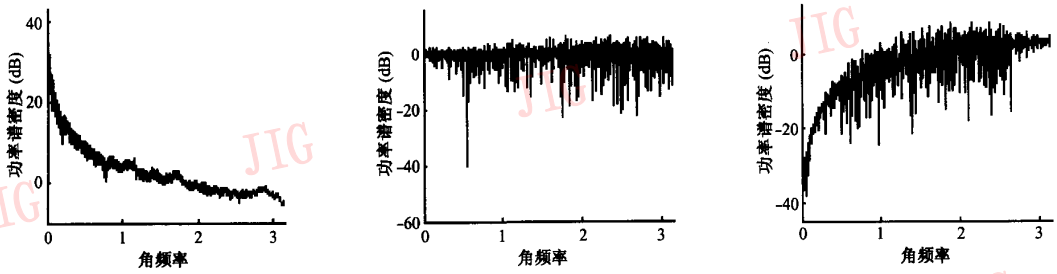
表 3　m 序列和 1 维 RLL 作为扩频码的比较

Tab. 3　Comparison between m-sequence and 1D-RLL sequence as spread spectrum code

图像	m 序列		1D-RLL 序列	
	$\overline{A^2_{cor}}$	$\eta(A_{cor})$	$\overline{A^2_{cor}}$	$\eta(A_{cor})$
Lena	12.9	15%	0.783	7.7%
Barbara	19.1	13%	3.43	8.2%
Boats	14.0	15%	0.961	6.5%
Bridge	18.7	13%	3.11	5.2%

由表 3 可以看出,使用 RLL 序列时,互相关系数样本二阶矩的均值减小到原来的 6 ~ 18%,这意味着水印嵌入强度可以减小到原来的 24 ~ 42%,相应的峰值信噪比可以提高 7 ~ 12dB;或者在不改变水印嵌入强度时,正确提取的水印比特数将从 68% 提高到 98.3 ~ 99.99%。同时发现,$\eta(A_{cor})$平均减小了 50% 以上,这说明了互相关系数的样本二阶矩方根对于不同序列的稳定性,也得到很大的改善。

图 1 显示了 1 维情况下,图像和扩频序列的功率谱。由该图可以看出,RLL 序列的高通特性正好和图像的低通特性相反。



(a) Peano 扫描并加三角窗的 Lena 图功率谱　(b) m 序列功率谱　(c) 1 维 RLL 序列功率谱

图 1　各序列的功率谱

Fig. 1　The power spectrum of sequences

应用先前提出的理论，不仅可以在频域解释 RLL 序列和图像的正交性更好的原因，也可以在空域解释。在 RLL 序列中，由于连号长度受限，因此前后相继的符号有很大的概率取不同的正负号，而在 m 序列中，因为符号间近似相互独立，取不同正负号的概率可以近似看作为 1/2，所以，对于较小的 $\|q\|$，RLL 序列的 $R(q)$ 比 m 序列的 $R(q)$ 要小。

事实上，由于 n 阶 m 序列共有 2^{n-1} 个游程[9]，因此，m 序列中满足后继比特和本身符号不同的比特数 $B_m = 2^{n-1} - 1$；而本文产生的 RLL 序列中，$B_{RLL} = 2^{n-1} + 2^{n-2} - 1$，远大于 B_m。由此可计算得到：$R_{RLL}(\pm 1) \approx -0.5$，而 $R_m(\pm 1) \approx 0$，这样乘以 $H(\pm 1) = 2^n - 1$ 后，两者就相差很大了。

3.2 2 维 RLL 扩频序列

对于 2 维的情形，可将 1 维中的 RLL 编码方法进行推广，即取一个 $n-2$ 阶的 m 序列，先按行折叠成 2 维矩阵形式，再将 0 映射成 $\begin{bmatrix} -1 & +1 \\ +1 & -1 \end{bmatrix}$，而将 1 映射成 $\begin{bmatrix} +1 & -1 \\ -1 & +1 \end{bmatrix}$。这样得到的 2 维序列在水平和垂直方向上游程长度都不会超过 2。

表 4 是分别使用 m 序列折叠成的 2 维序列和 2 维RLL 序列时，互相关系数的样本二阶矩的对比。实验时图像保持 2 维形态，其余实验条件同前。

表 4 m 序列和 2 维 RLL 作为扩频码的比较

Tab. 4 Comparison between m-sequence and 2D-RLL sequence as spread spectrum code

图像	折叠 m 序列		2D-RLL 序列	
	$\overline{A_{cor}^2}$	$\eta(A_{cor})$	$\overline{A_{cor}^2}$	$\eta(A_{cor})$
Lena	12.5	17%	0.252	6.6%
Barbara	18.7	19%	1.93	11%
Boats	14.4	17%	0.190	5.8%
Bridge	18.6	15%	1.45	5.0%

与表 3 比较可以看出，这种 2 维 RLL 序列比 1 维RLL 序列更能减小互相关系数的二阶矩，而稳定性两者近似。

4 结 论

由空域和频域的 $E[\gamma_{cor}^2]$ 的表达式可明确说明，常用的白噪声伪随机序列在和图像作相关运算时，其并不是最优的正交序列。这是因为自然图像通常是低通型的，而高通型的伪随机序列的频谱正好与之相反，其与白噪声序列在整个频带内都均匀平坦的频谱相比，高通型的序列显然与自然图像有更好的正交性，而这一点一直没有被人们所重视。由于本文提出的由 m 序列编码而来的 RLL 序列，恰好符合频谱高通的要求，因此比单纯的 m 序列有更好的正交效果。实验也证实了这一点。

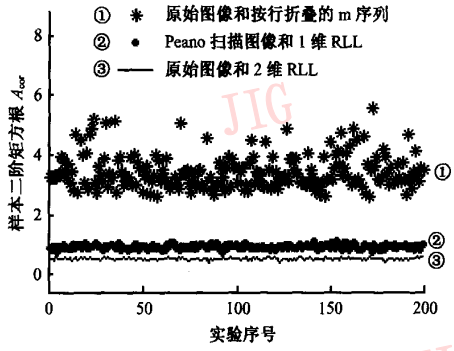


图 2 在 Lena 图上 3 种方法的比较

Fig. 2 Contrast among three different methods for Lena image

当然，从保密的角度而言，白噪声序列是最难被猜测的。在本文中表现为：从 m 序列调制生成 RLL 序列时，由于使用的 m 序列阶数降低，长度变短，因而此 m 序列更容易被猜测。当然，可以采用更复杂的编码方法来抑制这种阶数降低的程度，也可以采用高阶 m 序列的片段来生成 RLL 序列。实践证明，破译这些片段的难度和破译同阶全周期 m 序列的难度是基本相等的。

今后要研究的是，如何进一步提高序列与图像的正交性以及如何在保证正交性的前提下提高序列的保密性。

参考文献(References)

1 Tirkel A, Osborne C, Van Schyndel. Image watermarking-a spread spectrum application [A]. In: Proceedings of International Symposium on Software Testing and Analysis[C], Mainz, Germany, 1996: 785 ~ 789.

2 Hartung F, Girod B. Digital watermarking of raw and compressed video[A]. In: Proceedings of the SPIE Digital Computer Technology and Systems for Video Communication[C], Berlin, Germany, 1996: 205 - 213.

3 Hartun F, Girod B. Digital watermarking of MPEG-2 coded video in the bitstream domain [A]. In: Proceedings of International Conference on Acoustics, Speech, and Signal Processing [C], Munich, Germany, 1997: 2621 ~ 2624.

4 Zhong Hua, Liu Fang, Jiao Li-cheng. A blind meaningful wastermarking algorithem[J]. Journal of Image and Graphics, 2002,

7(10):1000~1004.[钟桦,刘芳,焦李成. 一种有意义水印盲提取算法[J]. 中国图象图形学报,2002,7(10):1000~1004.]

5 Wolfgang R, Delp E. A watermark for digital images[A]. In: Proceeding of International Conference on Image Processing[C], Lausanne, Switzerland, 1996:219~222.

6 Zhou Li-jun, Zhou Yuan-hua. Spatial domain image watermarking technology based direct sequence spread spectrum codes[J]. Journal of Software, 2002, **13**(2): 298~303.[周利军,周源华. 基于直接序列扩频码的图像空间域水印技术[J]. 软件学报,2002,**13**(2):298~303.]

7 Lian Qiu-sheng, Wang Cheng-ru. An watermark scheme based on chaos and the performance analysis[J]. Chinese Journal of Scientific Instrument, 2002, **23**(5):157~159.[练秋生,王成儒. 混沌数字水印及其性能分析. 仪器仪表学报[J]. 2002,**23**(5):157~159.]

8 Pratt W. Digital image processing(2nd ed.)[M]. New York: Wiley, Puldishers, 1991.

9 Lee J, Miller L. CDMA systems engineering handbook[M]. Norwood: Artech house publishers, 1998.

10 Lam E, Goodman J. A mathematical analysis of the DCT coefficient distributions for images[J]. IEEE Transactions on Image Processing, 2000, **9**(10):1661~1666.

11 Sheng Zhou, Xie Shi-qian, Pan Cheng-yi. Probability theory and mathematical statistics(2nd ed.)[M]. Beijing: Higher Education press, 1989:349.[盛骤,谢式千,潘承毅编. 概率论与数理统计(第2版)[M]. 北京:高等教育出版社,1989:349.]

12 Marusic B, Kale I, Tasic J. Image compression based on fast adaptive resampling on a Hilbert-Peano curve[A]. In: Proceedings of Instrumentation and Measurement Technology Conference[C], Venice, Italy 1999:156~159.

13 Immink. Runlength-limited sequences[J]. Proceedings of IEEE, 1990, **78**(11): 1745~1759.

14 Wells R. Applied coding and information theory for engineers[M]. Beijing: Engineering Industry Press, 2002: 77~81.

附　录

式(2)的证明:

对 $M\times N$ 矩阵 $\boldsymbol{f}$,矩阵左上角坐标为(0,0),右下角为(M,N),矩阵中的元素记为$f(x,y)$。

2D-DFT 定义为

$$F(u,v)=\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}f(x,y)\exp\left[-2\pi\mathrm{j}\left(\frac{ux}{M}+\frac{vy}{N}\right)\right]$$

2D-IDFT 为

$$f(x,y)=\frac{1}{MN}\sum_{u=0}^{M-1}\sum_{v=0}^{N-1}F(u,v)\exp\left[2\pi\mathrm{j}\left(\frac{ux}{M}+\frac{vy}{N}\right)\right]$$

因 2D-DFT 是酉变换,故可保持内积不变:

$$\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}f_1(x,y)f_2^*(x,y)=\frac{1}{MN}\sum_{u=0}^{M-1}\sum_{v=0}^{N-1}F_1(u,v)F_2^*(u,v)$$

本文中,$\boldsymbol{t}$ 和 $\boldsymbol{R}_{\mathrm{seq}}$ 均是关于(M,N)点对称的实矩阵,且矩阵的大小均为 $2M-1\times 2N-1$。因变换具有周期性,故可将它们周期延拓后,移位成关于(0,0)点对称的实矩阵 $\boldsymbol{t}_0$ 和 $R_{\mathrm{seq}}^{(0)}$,即,$t_0(x,y)=g(x+M,y+N)$,$R_{\mathrm{seq}}^{(0)}(x,y)=R_{\mathrm{seq}}(x+M,y+N)$。取以(0,0)为始点的一个周期,做 2D-DFT,得 $T_0(u,v)$ 和 $S_0(u,v)$。由变换定义式可证明:$\boldsymbol{T}_0$ 和 $\boldsymbol{S}_0$ 也是关于(0,0)点对称的实矩阵。

这样由保持内积的性质可得

$$\sum_{\boldsymbol{q}}t_0(\boldsymbol{q})R_{\mathrm{seq}}^{(0)}(\boldsymbol{q})=\frac{1}{(2M-1)(2N-1)}\times\sum_{\boldsymbol{p}}T_0(\boldsymbol{p})S_0(\boldsymbol{p})$$

上式中,$\boldsymbol{q}\triangleq(x,y)$,$\boldsymbol{p}\triangleq(u,v)$

因为,

$$T(u,v)=T_0(u,v)\exp\left[-2\pi\mathrm{j}\left(\frac{uM}{2M-1}+\frac{vN}{2N-1}\right)\right]$$

所以,$\|T(u,v)\|=\|T_0(u,v)\|=T_0(u,v)$

同理,$\|S(u,v)\|=S_0(u,v)$

因为,$\sum_{\boldsymbol{p}}T_0(\boldsymbol{p})S_0(\boldsymbol{p})=\sum_{\boldsymbol{p}}\|T(\boldsymbol{p})\|\cdot\|S(\boldsymbol{p})\|$

所以

$$\mathrm{E}[\gamma_{\mathrm{cor}}^2]=\sum_{\boldsymbol{q}}t(\boldsymbol{q})R_{\mathrm{seq}}(\boldsymbol{q})=\sum_{\boldsymbol{q}}t_0(\boldsymbol{q})R_{\mathrm{seq}}^{(0)}(\boldsymbol{q})=\frac{1}{(2M-1)(2N-1)}\sum_{\boldsymbol{p}}\|T(\boldsymbol{p})\|\cdot\|S(\boldsymbol{p})\|$$

证毕。