第37卷 第14期 计 算 机 工 程 2011年7月
Vol.37 No.14 Computer Engineering July 2011

·安全技术· 文章编号：1000—3428(2011)14—0120—03 文献标识码：A 中图分类号：TP391

一种基于扩频机制的数字图像水印算法

孙利杰，赵景秀，郑美珠，高 忠

(曲阜师范大学计算机科学学院，山东 日照 276826)

摘 要：提出一种基于扩频机制的数字图像水印算法。用伪随机序列作为扩频码，对原始水印信息进行周期延拓扩频和加密，在考虑人眼视觉特性的基础上，确定扩频水印在平稳小波变换域的嵌入位置和强度，扩频序列的选取决定了所选用的小波变换域最大系数的个数以及水印的密钥序列。实验结果表明，该算法具有较强的鲁棒性。

关键词：伪随机序列；周期延拓；平稳小波变换；扩频水印

Digital Image Watermark Algorithm Based on Spread Spectrum Mechanism

SUN Li-jie, ZHAO Jing-xiu, ZHENG Mei-zhu, GAO Zhong

(School of Computer Science, Qufu Normal University, Rizhao 276826, China)

【Abstract】This paper proposes a digital image watermark algorithm based on spread spectrum mechanism. It selects the pseudo random sequence modulation for the periodic sequence of continuation, and then encrypts. Taking into account the characteristics of human visual system, the positions and strengths of embedding into the original image which uses the same chip rate coefficients of the stationary wavelet transform domain are obtained. Selecting spread spectrum sequence determines the maximum coefficients of the wavelet transform domain and the key period sequence of watermark. Experimental results show that the algorithm has strong robustness.

【Key words】pseudo random sequence; periodic sequence of continuation; stationary wavelet transform; spread spectrum watermark

DOI: 10.3969/j.issn.1000-3428.2011.14.039

1 概述

随着网络规模的不断扩大和数字化技术的日渐成熟，网上各种数字化图书、报刊杂志、绘画、照片、音乐、歌曲及影视作品的数量也急剧增加。这些数字化产品和服务都可实现网络传送，不受时间空间限制，甚至无须物流传输，在交易和支付完成后，就可高效快捷地通过网络提供给客户。而网络的开放性和资源共享使得如何有效地保护网络数字化产品的版权成为一个重要问题，必须有行之有效的技术手段以防止数字化产品的篡改、假冒、剽窃和盗用等。数字水印技术就是为了解决这一问题而产生的[1]。数字水印是隐蔽通信和知识版权保护的一种重要方法，目前广泛采用的数字水印技术是扩频(spread spectrum)技术。文献[2]提出了扩频水印的思想，将水印信息用伪随机序列进行扩展，并隐藏于感知重要成分之中。因此，目前很多文献中采用伪随机序列对原始水印进行调制[3]。由于伪随机序列具有类似白噪声的统计特性，又具有周期性和规律性，这意味着它们是可以预知的。这对于同步来说是很重要的，因为扩展信号必须与解扩展的数据信号匹配才能正确地提取信息。

根据扩频和调制的手段不同，扩频方法有很多种类：(1)基于片率概念的扩频方法。文献[4]采用该方法进行扩频，该方案对原始信息按片率进行扩展后再用伪随机序列进行调制。(2)基于双伪随机序列的扩频方法。文献[5]采用了基于双伪随机序列的扩频水印生成方法。(3)基于伪随机序列周期延拓的扩频方法。文献[6]采用伪随机序列对原始水印进行周期延拓以覆盖整个载体。

本文的扩频采用周期延拓的思想，即先对原始水印信息进行伪随机序列周期延拓扩频，然后对扩频序列加密。由于此处伪随机序列作为提取原始信息的密钥，为了进一步提高安全性，不能采用短 m 序列，因此本文在采用 m 序列进行周期延拓扩频基础上采用加密方法。

平稳小波变换的特点表明它具有良好的空间方向选择性，与人的视觉特性十分吻合。与平移不变小波变换和冗余小波变换相比，平稳小波变换具有冗余、平移不变性的性质。与经典的正交离散小波变换相比，它能对连续的小波变换给出一种更为近似的估计，能消除信号重建时的吉布斯现象，使信号重建后更平滑，视觉质量更好。因此，本文提出的基于扩频机制的数字图像水印算法采用平稳小波变换。

2 伪随机序列周期延拓加密

2.1 伪随机序列周期延拓扩频方法

基于片率概念的直接序列扩频水印方案对原始信息按片率进行扩展后再用伪随机序列进行调制。实际上，人们也可以对伪随机序列进行周期延拓以覆盖整个载体，然后把双极性原始信息的每一位乘上各伪随机序列即可实现扩频。本文的扩频思想先对原始水印信息进行周期延拓扩展，然后对扩频序列加密。设原始信息为双极性二值序列，长度为 N，即：

$$m=\left\{m_i \middle| m_i \in \{-1,1\}, 0 \leqslant i \quad N-1\right\}$$

为了与前文一致，设要生成的水印序列长度为 $N\times cr$。为此，首先产生一个长度为 cr 的二值伪随机序列如下：

基金项目：山东省自然科学基金资助项目(ZR2009GM009)；山东省高校科技计划基金资助项目(J09LG34)

作者简介：孙利杰(1982－)，女，硕士研究生，主研方向：图像处理，数字水印；赵景秀，副教授；郑美珠、高 忠，硕士研究生

收稿日期：2011-01-13 **E-mail：**dpslj_good@126.com

$$p=\left\{p_j\middle|p_j\in\{1,-1\},0\leqslant j\quad cr-1\right\}$$

对该伪随机序列进行周期延拓，原始水印信息和扩展方式如图 1、图 2 所示。

1	-1	-1	1	-1	1

图 1　原始水印信息

1	-1	-1	1	-1	1
1	-1	-1	1	-1	1
1	-1	-1	1	-1	1
1	-1	-1	1	-1	1

图 2　基于片率 *cr*=4 的信息扩展

可得到扩展的伪随机序列：

$$s=\left\{s_j\middle|s_j=p_i,i=j\bmod(cr),0\leqslant j\quad N\times cr-1\right\}$$

2.2　基于密钥 *k* 的伪随机序列周期延拓加密

本文对上面经周期延拓得到的密钥序列 s 进行分组操作，用 80×80 像素的 qufu 商标作为嵌入水印即 N=6 400，cr=4，分成 100 组。把每一组密钥序列分成 left 和 right 相等的两部分，把分组后密钥的起始位视为迭代的起始密钥，迭代中前 20 次迭代时密钥循环右移 6 位，后 4 次迭代时密钥循环右移 2 位，这样就完成 left 部分的加密，而 right 部分的加密和 left 一致，不再重述。

为保证加密和解密的对称性，前 20 次迭代每完成一次都要交换 left 和 right 两者的值，交换后各自的次序保持不变，后 4 次迭代不交换两者的值，到此把 128 位 left 和 128 位 right 合并成 256 位的加密密钥序列 s'，后面各组以此类推，最后把经过加密的这 100 组序列结合在一起就得到经周期延拓扩频和加密的伪随机序列。

3　基于扩频机制的数字图像水印算法

3.1　水印的嵌入

水印的嵌入步骤如下：(1)选定作为水印的载体图像用 m 序列进行扩频，扩频思想是对伪随机序列进行周期延拓。(2)对周期延拓的密钥序列加密，其基本思想是采用变换的组合与迭代。(3)对原始宿主图像利用平稳小波变换分解，选择最大的 $N\times cr$ 个中频系数用来携带水印信息。(4)将扩频序列与原始宿主信息相乘就得到扩频信息并结合其他频域重构出水印图像。

3.2　水印的提取

水印的提取步骤如下：

(1)对嵌入的水印图像进行小波分解得到中频系数并选择 $N\times cr$ 个最大的系数。

(2)将选择的 $N\times cr$ 个最大的系数与扩频码相乘(其实是解扩)和解密(在这加密与解密的唯一不同是密钥的次序相反)。由于扩频码序列与原始宿主图像是相互独立的，因此，就可恢复出水印信息序列 y。y 可以通过比特检测器获得，令得到的序列为：

$$f(1),f(2),\mathrm{L}\ ,f(N\times cr)$$

$$y(j)=\begin{cases}0 & f(j)>0\\ 1 & f(j)<0\end{cases}$$

这样就得到了发送的水印信息序列：

$$y'(j)=\left\{y(j)\middle|j=1,2,\mathrm{L}\ ,N\times cr\right\}$$

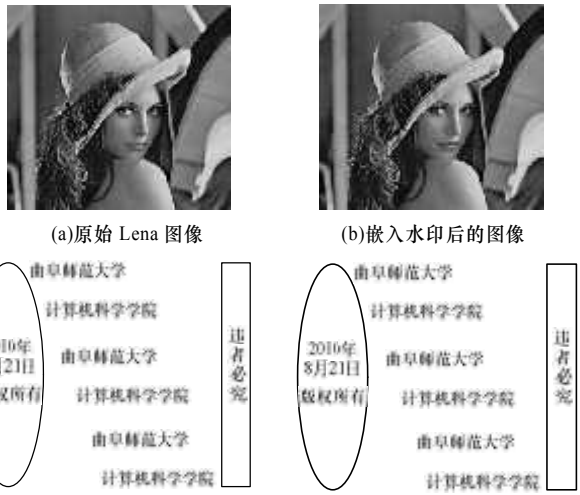
(3)计算归一化相关系数(*NC*)评价水印的检测效果：

$$NC=\frac{\sum_i\sum_j W(i,j)W^*(i,j)}{\sum_i\sum_j W(i,j)^2}=\begin{cases}\geqslant T & \text{存在水印}w\\ <T & \text{不存在水印}w\end{cases}$$

其中，T 是预先设定的阈值。经大量仿真实验验证，本文将 T 定义为 0.6。

4　仿真实验与分析

本文实验中仿真软件使用的是 Matlab7.0。原始宿主图像选用的是 256×256 像素的 Lena 图像。首先对原始宿主图像进行小波分解，选择 haar 小波基对原始图像 I(假设图像大小为 $M\times M$ 像素)进行 L 级小波分解。其中，L 取决于水印序列的长度 N，使得 $M\times\frac{M}{2^{2L}}\geqslant N$。本文通过实验选择 L=3 的 3 层小波分解，图像经小波分解后，子带图像 LL_L 集中了原始图像的绝大多数能量，为原始图像的逼近子图，稳定性好，尤其具有较好的抗压缩能力，但其视觉感知重要，再次嵌入水印后，不可见性差，水印嵌入的信息量少，所以将水印嵌入到边缘细节子带(LH_3, HL_3)中。实验结果表明，基于 LH_3 和 HL_3 子带的水印不可见性及抗剪切、平移能力较强。本文取 α=0.067。实验结果如图 3 所示，其中，图 3(b)显示的嵌入水印之后的载体图像的峰值信噪比为 41.791 dB。



(a)原始 Lena 图像　(b)嵌入水印后的图像

(c)原始水印图像　(d)提取的水印图像

图 3　扩频水印的嵌入和提取结果

数字水印算法的一个性能指标是水印的抗干扰能力。为此，本文对嵌入水印后的图像进行各种鲁棒性实验。实验中使用 1 000 组伪随机序列和嵌入的水印序列进行相关性检测，其中第 200 个序列为嵌入的水印序列。水印的抗干扰实验结果如图 4 所示。

(a)裁减 1/4

(b)图像向右平移 10 个像素　(c)图像向右平移 30 个像素

图 4　水印的抗干扰实验结果

图 5 是未经任何处理的嵌有水印图像的检测结果。对应图 4 中经过各种图像处理后的水印检测结果如图 6 所示。

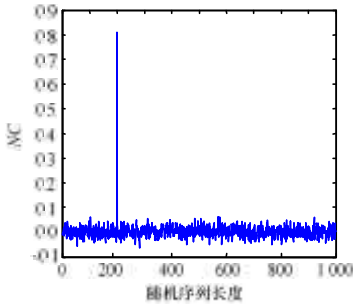
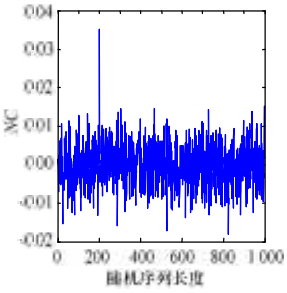
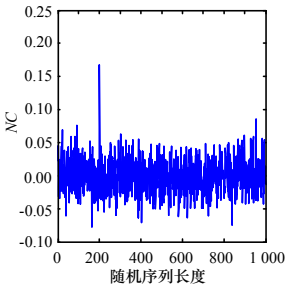


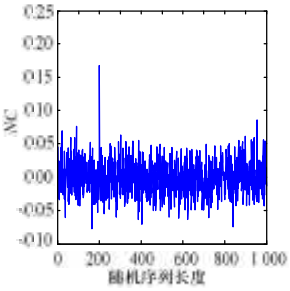
图 5 未经任何处理的嵌有水印图像的检测结果



(a)裁剪 1/4



(b)图像向右平移 10 个像素



(c)图像向右平移 30 个像素

图 6 图像处理的水印检测结果

可以看出，本文算法在椒盐噪声、高斯噪声、中值滤波、JPEG 压缩、裁剪时检测效果明显；但是在平移时当平移像素为 10 个、30 个时检测效果还比较显著，可见平稳小波变换在冗余、平移不变性上较有优势。可是当平移像素为 50 时几乎检测不到水印，可见本算法在平移时还是有局 限性。

5 结束语

本文提出一种基于扩频机制的数字图像水印算法，在扩频机制下利用平稳小波变换能使检测水印的鲁棒性和安全性得到提高。下一步的工作是改进本文算法在平移时的局限性，进一步提高混合变换域中数字图像水印抵抗各种几何攻击的鲁棒性。

参考文献

[1] Singhal N, Lee Young-Yoon, Kim Chang-Su, et al. Robust Image Watermarking Using Local Zernike Moments[J]. Journal of Vision Communication and Image Representation, 2009, 20(6): 408-419.

[2] Cox I J, Kilian J, Shamoon T, et al. Secure Spread Spectrum Watermarking for Multimedia[J]. IEEE Trans. on Image Processing, 1997, 6(12): 1673-1687.

[3] 许文丽，万 力，李 磊，等. 基于混沌置乱和混合变换域的扩频水印方案[J]. 计算机科学, 2007, 34(7): 248-250.

[4] Caccia G, Lancini R. Data Hiding in MPEG-2 Bit Stream Domain[C]//Proc. of EUROCON'01. [S. l.]: IEEE Press, 2001.

[5] Li Ying, Gao Xinbo, Ji Hongbing. A 3D Wavelet Based Spatial-temporal Approach for Video Watermarking[C]//Proc. of ICCIMA' 03. Xi'an, China: [s. n.], 2003.

[6] Vassaux B, Nguyen P, Baudry S, et al. Scrambling Technique for Video Object Watermarking Resisting to MPEG-4[C]//Proc. of VIPromCom'02. Zadar, Croatia: [s. n.], 2002.

编辑 顾姣健

(上接第 119 页)

$R_{1i}=(g_1)^{S_i} \bmod N$，$R_{2i}=(g_2)^{S_i} \bmod N$，这也可以看作是 P_i 执行了 RSA 算法的解密算法：N 为模数，S_i 为私钥，g_1、g_2 为密文，R_{1i}、R_{2i} 为明文，因此攻击者由 R_{1i}、R_{2i} 推导出 S_i 的难度也等价于破解出 RSA 体制中的用户私钥。

5 多秘密共享

本文方案在不更换参与者 P_i 的秘密份额 S_i 的情况下，只需 d 公布新的参数 g_1、g_2 以及重构新共享秘密所需的相应多项式的公开函数值，即可实现公平共享多个秘密。

任何人都不可能通过参与者 P_i 关于共享秘密 s 的公开信息 $\{S_{1i},S_{2i},R_{1i},R_{2i}\}$ 推导出其关于其他未重构的共享秘密 s' 的相关信息，即一个共享秘密的重构不会影响其他未重构秘密的安全性，这是由 RSA 算法的安全性保证的。

6 结束语

本文基于 RSA 密码体制和 Shamir 门限方案，提出了一个新的(v,t,n)公平秘密共享方案。方案具有以下性质：(1)秘密份额由各个参与者自己选择，其他人均不知道该份额；(2)即使系统中存在 $v(v<t/2)$个欺诈者，在重构秘密时，所有参与者仍然有同样的概率恢复出共享秘密；(3)每个参与者只需维护一个秘密份额就可以实现对多个秘密的共享；(4)方案的安全性基于 RSA 密码体制和 Shamir 门限方案的安全性。

参考文献

[1] Tan Kaijun, Zhu Hongwen, Gu Shangjie. Cheater Identification in (t,n) threshold Scheme[J]. Computer Communications, 1999, 22(1): 762-765.

[2] Tseng Yuh-Min. Multi-party Key Agreement Protocols with Cheater Identification[J]. Applied Mathematics and Computation, 2003, 145(2/3): 551-559.

[3] 庞辽军，王育民. 基于 RSA 密码体制(t,n)门限秘密共享方案[J]. 通信学报, 2005, 26(6): 70-73.

[4] 贺 军，李丽娟，李喜梅. 一种新的可验证多秘密共享方案[J]. 计算机工程, 2009, 35(9): 119-120.

[5] Laih C S, Lee Y C. V-fairness (t, n) Secret Sharing Scheme[C]// Proceedings of Conference on Computers and Digital Techniques. Stevenage, UK: [s. n.], 1997: 245-248.

[6] Hwang Ren-Junn, Chang Chin-Chen. Enhancing the Efficiency of (v,t,n) Fairness Secret Sharing Scheme[C]//Proceedings of the 18th International Conference on Advanced Information Networking and Application. [S. l.]: IEEE Press, 2004: 208-211.

编辑 张 帆