抗噪声、几何失真和 JPEG 压缩攻击的鲁棒数字水印方案

许文丽[①]　李　磊[①②]　王育民[①]
[①](西安电子科技大学 ISN 国家重点实验室　西安　710071)
[②](郑州大学信息工程学院　郑州　450052)

摘　要：该文提出了一个抗噪声、几何失真和 JPEG 压缩攻击的鲁棒数字水印方案，首先对原始水印信息进行置乱变换，然后再进行 Turbo 码编码以及扩频、合成，产生 CDMA 水印信息，在充分考虑人眼视觉特性的基础上确定编码水印在 DWT 和 DCT 混合变换域的嵌入位置和强度。为了减小水印提取过程中多址干扰(MAI)的影响，通过采用好的编译码方法(Turbo 码)降低接收机检测门限来实现。实验结果表明，应用该文提出的数字水印方案，水印的安全性有了很大提高，而且，在保证水印不可见的情况下，水印容量大大增加了。更重要的是，对剪切、平移、旋转等各种几何失真攻击以及噪音攻击、JPEG 压缩、滤波等常见的信号处理都具有极强的鲁棒性，即使嵌有水印的图像遭受攻击后质量损伤严重，水印图像还是能够清晰地提取出来。

关键词：数字水印；Arnold 置乱变换；Turbo 码；CDMA；混合变换
中图分类号：TP391　　**文献标识码**：A　　**文章编号**：1009-5896(2008)04-0933-04

Robust Digital Watermarking Scheme Resistant to Gaussian Noise, Geometric Distortion and JPEG Compression Attacks

Xu Wen-li[①]　Li Lei[①②]　Wang Yu-min[①]
[①](*National Key Laboratory of ISN*, *Xidian University*, *Xi'an* 710071, *China*)
[②](*Information Engineering College*, *Zhengzhou University*, *Zhengzhou* 450052, *China*)

Abstract: In this paper, a digital watermarking algorithm resistant to the noise, geometric distortion and JPEG compression is proposed. Firstly, in order to enhance the security of the watermarking, the original meaningful binary image watermarking is scrambled with using Arnold transform. Then the scrambled watermarking is encoded by using Turbo code and CDMA technology. Taking into account the characteristics of human visual system (HVS), the positions and strengths of embedding the image are obtained. In the process of watermarks extracting, there must be the influence of Multiple Access Interference (MAI). By taking advantages of good encoding method (such as Turbo code) to lower the threshold of receiver, the influence of MAI can be dropped. The experimental results show that the presented digital watermarking scheme is more secure，and at the same time, keeping the watermarking imperceptible, higher watermarking capacity can be embedded into host image. More important, it is robust against general image processing operations, especially against adding Gaussian noise, geometric distortion (including cropping, horizon moving and rotating), JPEG glossy compression, filter attacks. Even the watermarked image degraded greatly because of the attacks, the watermarking can be extracted very well.
Key words: Digital watermarking; Arnold scramble transform; Turbo code; CDMA; Hybrid transform

1　引言

数字水印是隐蔽通信和知识版权保护的一种重要方法，目前应用较多的是具有实际意义的水印信息(文本、图像、音频或视频)，这类水印的特点是水印信息数据量较大，相对而言，水印的不可见性就会减弱。而用于版权保护的数字水印则要求具有较强的鲁棒性，而数字水印的不可见性和鲁棒性本身就是一对矛盾，如果水印的数据量较大，这对矛盾就会更为显著。如何切实有效解决这一对矛盾呢？为此很多国内外专家学者从水印预处理、嵌入和提取等各方面提出了很多算法及改进方法，水印系统的鲁棒性确实得到了长足的发展。水印系统实际上是一个通信系统，作为版权或认证信息的水印，在载体信道中传输时，不可避免会受到各种有意无意攻击，所以在数字水印系统中应用纠错码技术来提高水印的鲁棒性是很必要的。目前，通信系统中的扩频技术被广泛应用于数字水印系统以增强其抗干扰性和保密性，COX 等人[1]最早提出了扩频水印的思想，即将水印信息用伪随机序列进行扩展，并隐藏于载体感知重要成分之中，从而提高了水印信息抗攻击特性。扩频水印具有鲁棒性强、高度保密的

2006-09-26 收到，2007-04-02 改回
国家自然科学基金(60473027)和“十一五”通信技术预研项目(110010203)资助课题

特性，但也有水印容量低的缺点。在通信系统中，码分多址CDMA(Code Division Multiple Access)，是一种有效的通信方式，CDMA 有诸多优点[2]，如抗噪声、抗干扰能力强，隐蔽性好，可多址复用，容量大等。因此将 CDMA 技术应用于水印系统中，既提高了水印的鲁棒性、安全性，还能够大大增加水印容量。

大量研究表明，利用 CDMA 技术在数字媒体中嵌入信息是一种实用、有效的方法。Vassaux 等人[3]提出在空间域将原始图像分成多层嵌入平面作为独立 CDMA 信道的水印技术并验证了算法的健壮性。Silvestre 等人[4]描述了扩频 CDMA 技术在 DCT 变换域内的水印方案。文献[5]在视频水印中应用了 CDMA 技术。国内，方艳梅[6,7] 、古利民[8]、朱岩[9]等人也从不同的方面将 CDMA 技术应用于数字水印中，并对其性能进行了分析。

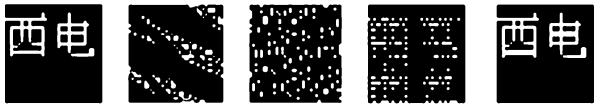
本文对置乱变换、Turbo 码编码和 CDMA 技术做了进一步研究和实验，分别利用它们优良的安全隐蔽性、纠错编码特性以及抗干扰大容量特性，基于 DWT 和 DCT 混合变换域，提出了抗噪声、几何失真和 JPEG 压缩攻击的鲁棒数字水印方案。实验结果表明，利用本文提出的数字水印方案，具有图像失真小、容量大、安全隐蔽性高的优点，而且水印系统对常见信号处理攻击的鲁棒性较强，尤其具有较强的抗噪声、几何失真(如剪切、平移、旋转)、JPEG 压缩和滤波等攻击能力。

本文第 2 节阐述了编码水印的产生，第 3 节提出了基于 DWT 和 DCT 混合变换域的鲁棒数字水印方案，第 4 节进行仿真实验和结果分析，最后总结全文。

2 基于 Turbo 码和 CDMA 的数字水印产生

2.1 水印置乱

为了消除水印图像中各像素之间的相关性，以增强水印信息的安全性和抗剪切处理等的鲁棒性，本文首先应用一个简单的传统混沌系统——猫映射(cat map)，对水印图像进行反复迭代变换，当遍布了水印图像所有像素点之后，便产生了置乱后的水印图像，这样水印图像得到了很好的保密预处理。下面给出原始水印图像和置乱后的图像如图 1 所示：



(a) 原始水印图像　(a1) 置乱 1 次　(a2) 置乱 10 次　(a3) 置乱 12 次　(a4) 置乱 24 次

图 1　32×32 的水印图像及其置乱后的图像

2.2 Turbo 码编码水印的生成

将原始水印信息 $\boldsymbol{w}=\{w_1,w_2,\cdots,w_N\}$ 进行置乱处理后得 $\boldsymbol{w}'=\{w_1',w_2',\cdots,w_N'\}$，对其进行 Turbo code 编码，本文采用的 Turbo 码是(7,5)的并行级联卷积码结构，两个递归系统卷积码的码率为 1/2，编码后，总的码率为 1/3，经过采用删余矩阵 $\boldsymbol{p}=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$ 后，码率就会提高到 1/2。这样，系统输出与校验比特复接后的码字序列为 $\boldsymbol{w}_{ecc}=\{w_1^{ecc},w_2^{ecc},\cdots,w_L^{ecc}\}$，其中 $L=2\times N+m$，N 表示原始水印信息序列长度，m 为编码存储长度。

2.3 CDMA 水印的生成

原始水印图像进行置乱变换和 Turbo 码编码后所形成的比特序列为 $\boldsymbol{w}_{ecc}=\{w_1^{ecc},w_2^{ecc},\cdots,w_L^{ecc}\}$，根据扩频增益因子和选取的可嵌入水印的宿主图像的系数个数来确定分组的大小，设每组 R 个元素，分成的组数 $K=\mathrm{ceil}(L/R)$，若第 K 组不足 R 个元素，则补“0”填充。在此可将 K 组看成是通信中的 K 个用户，第 i 个分组中的水印序列看成是第 i 个用户传输的信息：

$$g\{i\}=\{g_i(j)\in\{-1,1\}|j=1,2,\cdots,R\},\quad i=1,2,\cdots,K \tag{1}$$

设选用的准正交的随机码集为 $\boldsymbol{c}=\{c\{i\}|i=1,2,\cdots,K\}$，周期为 P。设 $g\{i\}$ 中码元宽度为 T_b，地址码的伪码码元宽度为 T_p，且取 $T_b=mT_p$，应用 CDMA 对水印信息进行编码得

$$\boldsymbol{S}=\sum_{i=1}^{K}s\{i\}=\sum_{i=1}^{K}g\{i\}c\{i\} \tag{2}$$

然后，将 $\boldsymbol{S}=\{S(i)|i=1,2,\cdots,M\}$，其中 $M=mR$，按照一定的嵌入规则嵌入到选取的载体混合变换域系数中。

3 基于 DWT 和 DCT 混合变换域数字水印方案

3.1 基于 DWT 和 DCT 混合变换域数字水印的嵌入

基于小波变换的图像多分辨率分解特点表明，它具有良好的空间方向选择性，与人的视觉特性十分吻合，但很少考虑数字图像经过小波变换后的各个子带图像中相邻小波系数之间存在着很强的相关性问题。相比较而言，离散余弦变换是实变换，具有很好的能量压缩能力和去相关能力。为此，本文结合离散小波变换的多分辨率特性和离散余弦变换的能量压缩能力以及解相关能力，在 DWT 和 DCT 结合的混合变换域嵌入水印，从而具有较好的抗 JPEG 压缩能力。

通过对原始宿主图像进行 DWT 三级分解，再对各子带进行 DCT 变换，并分别嵌入同量水印(32×32 的水印图像)进行抗攻击性能实验，限于篇幅，只给出试验结论：图像分解的层数越多，嵌有水印图像的不可见性和鲁棒性越强；综合各子带实验结果表明，cH3 子带不可见性较好，抗各种攻击能力较强。所以本文选取 cH3 子带(64×64)，再对其进行 DCT 变换，利用常用的加性嵌入公式，将上节编码水印 $\boldsymbol{S}$ 嵌入到原始宿主图像中：

$$X_i^w=X_i+\alpha_i S(i),\ i=1,2,\cdots,M \tag{3}$$

其中

$$S(i)=\sum_{j=1}^{K} g\{j\}(i')\times c\{j\}(i) \tag{4}$$

式中 $\boldsymbol{X}=\{X_i\}$ 为选取的要嵌入水印信息的宿主图像的 DWT 和 DCT 混合变换域系数集，$\boldsymbol{X}_w=\{X_i^w\}$ 为嵌入水印后的宿主图像系数集，α_i 是水印的嵌入强度。最后，再利用相应系数进行逆离散余弦变换 IDCT 和逆离散小波变换 IDWT，就得到了嵌有水印的图像 I_w：$I_w=\mathrm{IDWT}(\mathrm{IDCT}(X^w))$。

3.2 CDMA 水印的提取和检测

首先将接收机接收到的嵌有水印信息的图像 I'_w 进行 DWT 变换，根据密钥找出 cH3 子带，再对其进行 DCT 变换，然后根据水印长度和嵌入的位置密钥，找出嵌有水印的系数 $\boldsymbol{x}^{wn}=\{x_i^{wn}\}$，$x_i^{wn}=x_i^w+n_i,\quad i=1,2,\cdots,M$（$n_i$ 是指在传输过程中受到的噪声攻击），将 $\boldsymbol{x}^{wn}$ 分别与伪码序列 $c\{1\}$, $c\{2\},\cdots,c\{K\}$ 相乘，由于伪码序列与原始宿主图像是相互独立的，并且伪码序列之间是准正交的，这样，就可恢复出各组水印信息 $g\{1\},g\{2\},\cdots,g\{K\}$。实际上，比特检测器将 $\boldsymbol{x}^{wn}\cdot\boldsymbol{c}\{i\}$ 的波形，每隔 T_b 积分一次，得到序列：$y_i(1)$, $y_i(2),\cdots,y_i(R)$，令

$$g'_i(j)=\begin{cases}0, & y_i(j)\le 0\\ 1, & y_i(j)>0\end{cases} \tag{5}$$

这样，就得到了各用户发送的水印序列：

$$g'\{i\}=\left\{g'_i(j)\middle|j=1,2,\cdots,R\right\},\quad i=1,2,\cdots,K \tag{6}$$

得到 $\boldsymbol{g}'=\{g'\{1\},g'\{2\},\cdots,g'\{K\}\}$ 后，将其合并，就得到了 Turbo 码编码后的水印信息序列 $\boldsymbol{w}'_{ecc}=\left\{w_1^{ecc'},w_2^{ecc'},\cdots,w_L^{ecc'}\right\}$。

将 Turbo 码编码后的水印信息 $\boldsymbol{w}'_{ecc}$ 交给 Turbo 码译码器进行译码，在 Turbo 码迭代译码算法中，尽管 MAP 算法比较复杂，但从译码性能上讲，MAP 算法是最好的[10]，所以本文采用了 MAP 译码算法。经过多次迭代后得到待测水印的最佳估值序列 $\boldsymbol{w}''=\left\{w''_1,w''_2,\cdots,w''_N\right\}$。最后，将 $\boldsymbol{w}''$ 进行反置乱变换就得到了提取出的原始版权水印信息的最佳估值序列 $\widehat{\boldsymbol{w}}=\left\{\widehat{w}_1,\widehat{w}_2,\cdots,\widehat{w}_N\right\}$。

4　仿真实验结果

本文实验中，原始宿主图像选用的是 512×512 的 lena 灰度图像，用小波基“haar”对 lena 图像进行 3 层小波分解，再对第 3 层水平细节分量 cH3 进行 DCT 变换，采用加性规则嵌入编码水印。

本文采用的准正交伪随机码 $c\{1\},c\{2\},\cdots,c\{K\}$ 为同一 m 序列的不同偏置，这正是利用了 m 序列优良的自相关特性。为了验证本文提出的水印系统的容量特性和抗攻击的鲁棒性能进行了如下两组实验。

实验 1　数字水印方案的容量实验

该实验所用水印图像是黑白二值图像，大小分别为：32×32，64×64，128×128，分组大小为 16×16，扩频增益因子分别为 15，实验结果如图 2 所示。

图 2　水印系统容量实验

实验结果表明，即使 128×128 大小的水印图像经 Turbo code 编码后变成 128×128×2+m 大小的水印信息序列，应用本文提出的算法，将其嵌入到 64×64 的 DWT 和 DCT 混合变换域子带系数上，嵌有水印的图像的视觉质量没有发生变化，尽管提取出的水印噪音较大，但水印图像还是很清晰的。

实验 2　数字水印方案的性能实验。对嵌有水印的图像进行噪声、滤波、几何失真、旋转、JPEG 压缩等攻击，并提取水印，实验结果如图 3 所示。

实验结果表明，本文提出的数字水印方案具有极强的抗噪声、几何失真(旋转、平移、剪切等)、JPEG 压缩以及滤波等攻击的鲁棒性能。

5　结束语

本文提出了一个抗噪声、几何失真和 JPEG 压缩攻击的鲁棒数字水印方案，通过在 DWT 和 DCT 混合变换域应用该方案，水印信息的安全隐蔽性得到了很大提高，而且在保证嵌入的水印的不可见性的情况下，大大提高了水印系统的容量。更重要的是，对几何失真攻击(如剪切、平移、旋转等)以及常见的信号处理攻击(如噪音，JPEG 压缩，滤波等)都具有很强的鲁棒性。

图 3 本文提出的数字水印系统的抗攻击性能比较

参 考 文 献

[1] Cox I J, Kilian J, Leighton T, and Shannon T. Secure spread spectrum watermarking for multimedia [J]. *IEEE Transaction on Image Processing*, 1997, 6(12): 1673−1687.

[2] 窦中兆, 雷湘等. CDMA 无线通信原理 [M]. 北京: 清华大学出版社, 2004, 2: 229−241.
Dou Zhong-zhao and Lei Xiang, *et al*. CDMA Radio Communications Principles[M]. Beijing: Tsinghua University Press, 2004, 2: 229−241.

[3] Vassaux B, Bas P, and Chassery J M. A new CDMA technique for digital image watermarking, enchancing capacity of insertion and robustness[A]. Proc. of IEEE Int. conf. on Image processing. Thessalonica, Greece. 2001, 3: 983−986.

[4] Silvestre G C M and Dowling WJ. Embedding data in digital images using CDMA techniques [A]. In: proceedings of IEEE international conference on Image processing, 2000, 1: 589−592.

[5] Bijan BM. Exploring CDMA for watermarking of digital video [A]. In: Proceedings of SPIE-The International Society for Optical Engineering, 1999, 3657: 96−102.

[6] Fang Yanmei, Huang Jiwu, and Wu Shaoquan. CDMA-Based watermarking resisting to cropping [A]. Proc. 2004 IEEE Int. sym. On Circuits and Systems [C]. ISCAS'04, Vancouver, Canada, May 2004, 2: 25−28.

[7] 方艳梅, 谷利民, 黄继武. 利用边信息嵌入的 CDMA 水印信道性能研究[J]. 电子学报, 2006, 34(1): 45−50.
Fang Yan-mei, Gu Li-min, and Huang Ji-wu. Performance analysis of CDMA-Based watermarking channel with side-information embedding [J]. *Acta Electronica Sinica*, 2006, 34(1): 45−50.

[8] 谷利民, 方艳梅, 黄继武. 基于叠加嵌入的码分多址数字水印信道性能分析[J]. 计算机学报, 2005, 28(2): 268−273.
Gu Li-min, Fang Yan-mei, and Huang Ji-wu. Performance analysis of CDMA watermarking channel using additive embedding [J]. *Chinese Journal of Computers*, 2005, 28(2): 268−273.

[9] 朱岩, 孙中伟, 杨永田, 冯登国. 扩频CDMA水印性能分析及其多小波域内的应用研究[J]. 计算机学报, 2005, 28(8): 1376−1385.
Zhu Yan, Sun Zhong-wei, Yang Yong-tian, and Feng Deng-guo. Performance analysis of spread spectrum CDMA watermarking and applied research in multiwavelet domain [J]. *Chinese Journal of Computers*, 2005, 28(8): 1376−1385.

[10] 刘东华等. Turbo 码原理与应用技术[M]. 北京: 电子工业出版社, 2004, 1: 79−82.
Liu Dong-hua. Turbo code principles and application [M]. Beijing: Publishing House of Electronics Industry, 2004, 1: 79−82.

许文丽： 女，1970 年生，博士，研究方向为数字水印.

李 磊： 男，1974 年生，博士，研究方向为网络安全.

王育民： 男，1936 年生，教授，博士生导师，主要研究方向为长期从事信息论、编码、密码学、语音加密、信息隐藏等方面的科研工作.