基于混沌置乱和混合变换域的扩频水印方案*)

许文丽　苏万力　李　磊　王育民
(西安电子科技大学 ISN 国家重点实验室　西安 710071)

摘　要　本文基于混沌置乱和 DWT 和 DCT 混合变换域提出了一种扩频数字水印方案，首先对原始水印信息进行混沌置乱预处理，然后应用扩频技术，选取 m-序列作为扩频码，对置乱预处理后的水印信息进行扩频，产生扩频水印信息，在充分考虑人眼视觉特性的基础上确定扩频水印在 DWT 和 DCT 混合变换域的嵌入位置和强度，扩频增益因子的选取大小取决于所选用的 DWT 和 DCT 混合变换域系数的个数以及水印大小。实验结果表明，应用文中提出的基于混沌置乱和混合变换域的扩频水印方案，不但水印的安全性有了很大程度提高，而且对剪切、旋转等各种几何失真攻击和常见的信号处理如噪音、JPEG 压缩和滤波攻击具有很强的鲁棒性，即使嵌有水印的图像遭受攻击后受损较严重，水印信息还是能够完好地提取出来。

关键词　数字水印，混沌置乱，扩频水印，离散小波变换(DWT)，离散余弦变换(DCT)

Spread Spectrum Watermarking Scheme Based on Chaos Scramble and Hybrid Transform Domains

XU Wen-Li　SU Wan-Li　LI Lei　WANG Yu-Min
(National Key Laboratory of ISN , Xidian University, Xi'an 710071)

Abstract　In this paper, a robust spread spectrum digital watermarking algorithm based on chaos scramble and hybrid transform domains is proposed. Firstly, in order to enhance the security of the watermarking, the original meaningful binary image digital watermarking is scrambled by using Arnold transform. Then the scrambled watermarking is spread by using spread spectrum technology. Taking into account the characteristics of human visual system (HVS), the positions and strengths of embedding into coefficients of the hybrid DWT and DCT domain are obtained. Selecting spread spectrum gain factor is determined by chosen coefficients of hybrid DWT and DCT domain and watermarking size.

The experimental results show that the presented chaos scramble and hybrid transform based spread spectrum digital watermarking algorithm is more secure and robust against geometric distortions (such as cropping, rotating and so on) and general image processing operations (such as adding Gaussian noise, JPEG glossy compression, filters). Though the quality of the watermarked image is seriously degraded because of the attacks , the watermarking can be extracted very well.

Keywords　Digital watermarking, Chaos scramble, Spread spectrum watermarking, Discrete wavelet transform, Discrete cosine transform

1　引言

数字水印作为数字产品版权保护的一种重要方法，近年来得到了长足的发展。数字水印系统，实际上是一个通信系统，作为版权或认证信息的水印则为在载体信道中传输的信号。水印信息可分为无意义水印和有意义水印，无意义水印虽然信息量小，但实际应用价值不大，所以常常应用有意义水印作为版权认证信息。在信息隐藏之前，如果先对秘密信息按照一定的运算规则进行置乱处理，使其失去原有的面目，然后将其隐藏到载体信息里面，这样我们所要传输的水印信息就更安全了。所以为了保证水印信息的安全保密性和抗剪切攻击能力，很有必要对水印信息进行伪随机化、置乱、扩频、位分解、编码或多种技术相结合的预处理操作。

关于图像置乱的研究已有很多[1~4]，常用的方法有：基于混沌系统、基于 Hilbert 曲线、基于 Arnold 变换、基于幻方矩阵、基于随机数的方法以及多种置乱算法相融合的方法等。

在通信系统中，扩频技术[5]是最早应用在军事通信中作为具有很强的抗干扰性的通信手段。直扩系统对窄带干扰、宽带干扰等，都具有很好的抗干扰能力，而且其抗干扰能力随着扩频处理增益的增加而增强。在直扩系统中，信号的检测概率与信号能量与噪声功率谱密度之比成正比，与信号的频带宽度成反比。由于扩频信号在很宽的频带上被扩展了，信号功率谱密度很低，这样，信号被湮没在噪声里，一般接收机发现不了直扩信号的存在，故而其隐蔽性很好；同时，直扩系统的抗衰落、抗多径干扰能力也很强。COX 等人[6]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。大量研究表明，扩频水印具有鲁棒性强、高度保密的特性。

文[7]阐明，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。所以 DWT 系数不具有几何不变性，那么嵌入到 DWT 域的水印也就不具有抗几何失真攻击(如剪切、旋转、移位等)能力。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。那么嵌入到 DCT 域的水印抗 JPEG 压缩和几何失真攻击的能力较强。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 相结合的混合变换域嵌入水印信息。

在本文中，作者提出了基于混沌置乱和混合变换域的扩频数字水印方案，首先对原始水印图像进行混沌置乱预处理，

*)基金项目："十一五"军事通信技术预研项目(110010203)。许文丽　博士。

然后应用扩频技术产生扩频水印，根据加性嵌入规则将扩频水印嵌入到选取的混合变换域系数上，结合信号系统和相关检测理论，提出了一种相关检测器。通过大量的实验和比较研究，结果表明，文中所提出的基于混沌变换和混合变换域的扩频数字水印系统具有图像失真小、鲁棒性强、安全隐蔽性高的优点。

本文第 2 节阐述了原始水印图像的混沌置乱过程，第 3 节阐述了扩频通信的理论基础和原理，并应用扩频技术对置乱预处理后的水印进行扩频，产生扩频水印，第 4 节提出了基于 DWT 和 DCT 混合变换域的扩频数字水印方案，第 5 节进行仿真实验和结果分析，最后总结全文。

2 数字水印的混沌置乱

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保密性和抗剪切处理等的鲁棒性，我们首先应用一混沌系统一猫映射(cat map)，也称 Arnold 变换，主要是利用图像的矩阵形式对图像信息进行置乱变换：

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \left[\begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \right] \bmod N, (x,y) \in \{0,1,\cdots,N-1\} \tag{1}$$

反复进行这一变换，可得到迭代程序：

$$p_{x',y'}^{n+1} = A p_{x,y}^{n} (\bmod N) \tag{2}$$

利用上式对水印图像中的各像素点坐标做变换，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，该变换是 Arnold 在遍历理论研究中提出的，具有周期性。将置乱后的图像按“Z”字形扫描，得到由 0，1 组成的二值序列，这样水印图像得到了很好的保密预处理，提高了数据的安全性和保密性，而且还可以恢复原始水印图像。下面给出了水印图像进行不同置乱次数后的置乱图像，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 原始水印图像和置乱后的水印图像

3 数字信号直接序列扩频(DS-SS)系统

3.1 扩频通信的理论基础

由信息论的基本知识可得，在高斯白噪声时，信道容量满足下式，即山农(shannon)公式：

$$C = B\log_2(1+\frac{S}{N}) \tag{3}$$

式中，c 为信道容量，单位为 b/s；B 为信号频带宽度，单位为 Hz；S 为信号平均功率，单位为 W；N 为噪声平均功率，单位为 W。

山农公式说明，在给定信号功率 S 和白噪声功率 N 的情况下，只要采用某种编码系统，就能以任意小的差错概率，以接近于 C 的传输速率来传送信息。在保持信息传输速率 C 不变的条件下，频带 B 和信噪比是可以互换的。也就是说，如果增加信号频带宽度，就可以在较低的信噪比的条件下以任意小的差错概率来传输信息，甚至在信号被噪声湮没的情况下，即 $S/N<1$ 或 $10\log_2 S/N<0$ dB，只要相应地增加信号带宽，也能进行可靠的通信。扩频通信的优越性在于用扩展频谱的方法可以换取信噪比上的好处。柯捷尔尼可夫(Котельников)在其潜在抗干扰性理论中得到如下关于信息传输差错概率的公式：

$$P_e \approx f(\frac{E}{n_0}) \tag{4}$$

公式指出，差错概率 P_e 是信号能量 E 与噪声功率谱密度 n_0 之比的函数。设信息持续时间为 T，或数字信息的码元宽度为 T，则信息带宽 B_m 为：

$$B_m = \frac{1}{T} \tag{5}$$

信号功率 S 为：

$$S = \frac{E}{T} = EB_m \tag{6}$$

已调(已扩频)信号的带宽为 B，则噪声功率为：

$$N = n_0 B \tag{7}$$

将式(3)～(5)带入式(2)，可得：

$$P_e = f\left(\frac{ST}{N} \cdot B\right) = f\left(\frac{S}{N} \cdot \frac{B}{B_m}\right) \tag{8}$$

上公式指出，差错概率 P_e 是输入信号与噪声功率之比 S/N 和信号带宽与信息带宽之比 B/B_m 二者乘积的函数，信噪比与带宽是可以互换的，同样指出了用增加带宽的方法可以换取信噪比上的好处这一客观规律。

理论分析表明，各种扩频系统的抗干扰能力大体上都与扩频信号带宽 B 与信息带宽 B_m 之比成正比，工程上常以分贝(dB)表示扩频系统的处理增益：

$$G_P = 10\log\frac{B}{B_m} \tag{9}$$

因为通信系统要正常工作，还需要保证输出端有一定的信噪比，我们常用抗干扰容限 M_j 来说明系统在干扰环境下的工作性能：

$$M_j = G_P - [(S/N)_O + L_s] \tag{10}$$

式中，$(S/N)_O$ 为输出端的信噪比；L_s 为系统损耗。

3.2 直接序列扩频(DS-SS)原理

所谓直接序列扩频就是直接用具有高速率的扩频码序列在发端去扩展信号的频谱，而接收端用相同的扩频码序列进行解扩，把展宽的扩频信号还原成原始信息。本文采用码序列与波形相对应的负逻辑关系[1]：即“0”用“+1”表示，“1”用“−1”表示，也就是，正脉冲代表“0”，负脉冲代表“1”，采用负逻辑关系时，序列的模 2 加与波形相乘是等效的，它们的关系是：

$$0 \oplus 0 = 0 \Leftrightarrow 1\times 1 = 1, 0 \oplus 1 = 1 \Leftrightarrow 1\times -1 = -1, 1 \oplus 0 = 1 \Leftrightarrow -1\times 1 = -1, 1 \oplus 1 = 0 \Leftrightarrow -1\times -1 = 1$$

3.3 直扩系统主要性能

直扩系统最早的应用是在军事通信中作为具有很强的抗干扰性的通信手段。直扩系统对窄带干扰、宽带干扰等，都具有抗干扰能力，其抗干扰能力大小就是前面提到的扩频处理增益 G_P，G_P 越大，抗干扰能力就越强。理论分析表明，信号的检测概率与信号能量与噪声功率谱密度之比成正比，与信号的频带宽度成反比。由于扩频信号在很宽的频带上被扩展

了，信号功率谱密度很低，这样，信号被湮没在噪声里，一般接收机发现不了直扩信号的存在，故而，其隐蔽性较好；同时还具有抗衰落、抗多径干扰能力强等特性。

扩频水印的生成过程如图 2 所示。

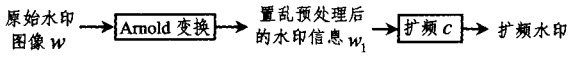

图 2　扩频水印的生成过程

设选用的随机码为 $c=\{c(i)\mid i=1,2,\cdots M\}$，周期为 P，且取 $T_b=mT_p$，应用 CDMA 对水印信息进行编码得：

$S=\{s(i)\mid i=1,2,\cdots,M\}=\{g(i)c(i)\mid i=1,2,\cdots,M\}$，其中 $M=mN$　　(11)

其中，N 为原始水印图像序列的长度，M 为扩频水印序列的长度。

4　基于 DWT 和 DCT 混合变换的数字水印方案

4.1　基于 DWT 和 DCT 混合变换的数字水印嵌入

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。所以 DWT 系数不具有几何不变性，那么嵌入到 DWT 域的水印也就不具有抗几何失真攻击（如剪切、旋转、移位等）能力。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。那么嵌入到 DCT 域的水印抗 JPEG 压缩和几何失真攻击的能力较强。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 相结合的混合变换域嵌入水印信息。

首先对原始宿主图像进行小波变换：选取适当的小波基对原始图像 I（假设图像大小为 $M\times M$）进行 L 级小波分解，其中 L 取决于水印序列的长度 N 使得 $M\times\frac{M}{2^{2L}}\geqslant N$。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，尤其具有较强的抵抗压缩的能力。但其视觉感知重要，在此嵌入水印，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，HL，HH）中。

我们知道，图像分解的层数越大，水印的不可见性和鲁棒性就越强。实验结果表明，基于 $cH3$ 子带的水印不可见性及抗攻击能力较强。所以本文选择将置乱后的水印序列嵌入到基于 $cH3$ 子带的 DWT 和 DCT 相结合的混合变换域系数上，水印嵌入采用常规的加法嵌入规则：

$$X_i^w=x_i+\alpha_i S(i),i=1,2,\cdots,M \qquad (12)$$

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：$I_w=IDWT(IDCT(X^w))$，水印嵌入过程如图 3 所示。

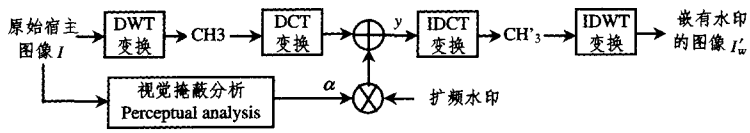

图 3　水印的嵌入过程

4.2　数字水印的提取和检测

扩频水印的提取过程，如图 4 所示。

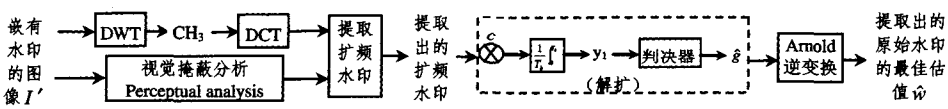

图 4　扩频水印提取过程

首先将接收机接收到的嵌有水印信息的图像 I'_w 选择相同的小波基进行三层 DWT 变换，根据水印长度和嵌入的位置密钥，找出嵌有水印的系数 $x_i^{wn}=x_i^w+n_i,i=1,2,\cdots,M$（$n_i$ 是指在传输过程中受到的噪声攻击），将 x^{wn} 与扩频码序列 c 相乘（实质是解扩），由于扩频码序列与原始宿主图像是相互独立的，这样，就可恢复出水印信息序列 g。实际上，比特检测器将 $x^{wn}\cdot c$ 的波形，每隔 T_b 积分一次（求和），得到序列：$y(1),y(2),\cdots,y(N)$，

令

$$g'(j)=\begin{cases}0,y(j)<0\\1,y(j)>0\end{cases} \qquad (13)$$

这样，就得到了发送的水印信息序列：$g'=\{g'(j)\mid j=1,2,\cdots,N\}$。

若对提取出的水印信息进行版权检测，可根据提取出的水印信息和原始水印信息的归一化互相关系数作为客观评价标准：

$$NCC=\frac{\sum_{i=1}^{N}w_i\hat{w}_i}{\sqrt{\sum_{i=1}^{N}w_i^2}\sqrt{\sum_{i=1}^{N}\hat{w}_i^2}}\begin{cases}\geqslant T\text{ 存在水印 }w\\<T\text{ 不存在水印 }w\end{cases} \qquad (14)$$

式中，T 是预先设定的阈值，经大量实验，我们将 T 的值定为 0.6。

5　仿真实验结果

本文实验中，原始宿主图像选用的是常用的 512×512 的 lena 灰度图像，用小波基“haar”对图像进行三层小波分解，并对其水平分量 CH3 进行 DCT 变换，原始水印图像采用的扩频码为序列，扩频增益因子为 $R=4$。基于混沌置乱和混合变换域的扩频水印系统的抗攻击性能如图 5 所示。

该实验结果表明，基于混沌置乱和混合变换域的扩频水印系统的抗各种攻击的鲁棒性极强，即使嵌有水印的图像遭受攻击后受损较严重，仍能够提取出完好的水印信息。

结论　本文提出了基于混沌置乱和混合变换域的扩频水印方案，正是利用了扩频技术所具有的抗干扰和噪声能力强、保密性好的优点，通过在 DWT 和 DCT 混合变换域应用该方法，水印信息的安全保密性得到了大大提高，对剪切、旋转等几何变换以及常见的信号处理攻击都具有很强的鲁棒性。

（下转封四）

（上接第 250 页）

图 5　基于混沌置乱和混合变换域的扩频水印系统的抗攻击性能比较

参 考 文 献

1　Frey D R. Chaotic digital encoding: an approach to secure communication[J]. IEEE Trans. on CAS-II, 1993, 40(10): 660～666

2　Voyatzis G, Pitas I. Digital image watermarking using mixing systems[J]. Compute & Graphics, 1998, 22(3): 405～416

3　孙锬，温泉，王树勋. 基于人类视觉的混沌阵列在图像上的水印算法[J]. 电子学报，2003，31(1)：149～153

4　张贵仓，王让定，张毓晋. 基于迭代混合的数字图像隐藏技术[J]. 计算机学报，2003，26(5)：569～575

5　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

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

7　孙圣和，陆哲明，牛夏牧. 数字水印技术与应用[M]. 科学出版社，2004

计算机科学

（1974 年 1 月创刊）

第 34 卷第 7 期（月刊）

2007 年 7 月 25 日出版

国际标准连续出版物号 ISSN 1002－137X

国内统一连续出版物号 CN50—1075/TP

定价：30.00 元　国外定价：5 美元

邮发代号：78—68

发行范围：国内外公开

主管单位：国家科学技术部

主办单位：国家科技部西南信息中心

编辑出版：《计算机科学》杂志社

重庆市渝北区北部新区洪湖西路 18 号　邮政编码：401121

电话：（023）63500828　E-mail：jsjkx@swic.ac.cn

网址：www.jsjkx.com

社　　长：牟炳林

总　　编：彭　丹

主　　编：朱宗元

主编助理：徐书令

印 刷 者：重庆科情印务有限公司

总发行处：重庆市邮政局

订 购 处：全国各地邮政局

国外总发行：中国国际图书贸易总公司（北京 399 信箱）

国外代号：6210—MO