《信息安全技术》课程考察

1. 请实现 RSA 算法的加密和解密算法，使之能适用于 1 千比特长的大整数加解密。并利用中国剩余定理加速 RSA 解密算法的计算速度，比较加速前后的 RSA 解密时间。

2. 图像数字水印技术有两类经典的水印嵌入算法。即扩频水印算法和量化索引调制方法。请任选下面一种算法实现：1）一种变换域上的扩频水印嵌入算法；2）一种量化索引调制水印嵌入算法。

参考文献

[1] 数字水印技术及应用，孙圣和、陆哲明、牛夏牧 著 / 科学出版社 / 2004

[2] Shinde, G. N., and H. S. Fadewar. "Faster RSA algorithm for decryption using Chinese remainder theorem." ICCES: International Conference on Computational & Experimental Engineering and Sciences. Vol. 5. No. 4. 2008.

请完成上面两道题，编写代码，撰写实验报告，并录制程序运行过程和结果的视频。将代码、报告、录屏这三个一起打包后发至 815694609@qq.com。

截止时间 2022 年 6 月 30 日星期四 11:59PM，过期不侯。

2.3.2 扩频水印生成方法

在实际应用中，原始信息往往是一组由{0,1}、{−1,1}或者{−c,c}组成的能代表数字产品版权信息的ID序列号(这里c是正整数)，它未必具有伪随机特性。为了扩展原始

信息的能量谱，该窄带信息可被一个宽带伪随机噪声序列发生器所调制(图2-9)，调制后的ID序列就可作为水印嵌入到数字产品之中[234]。调制时，原始版权信息的位数较少(有时只有64比特)，而伪随机噪声序列的周期很长，这样就达到了扩频目的，通常称之为扩频调制(spread spectrum modulation)，属于直接序列扩频方式。下面，根据扩展和调制手段的不同，分别介绍各种扩频方法。

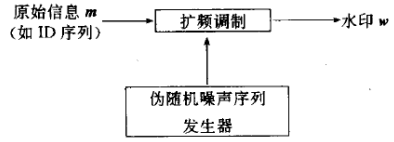

图2-9　基于直接序列扩频原理的数字水印生成

1. 基于片率(chip rate)概念的扩频方法

基于片率概念的直接序列扩频水印方案首先由Hartung和Girod等[69,228,235]提出，随后很多文献中均采用该方法进行扩频[60~63,68~70,195,198]。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，其原理如图2-10所示。

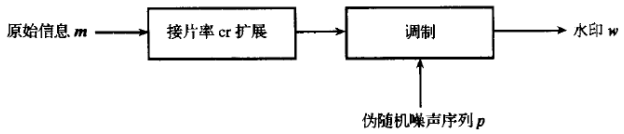

图2-10　基于片率概念的扩频水印生成

设原始信息为双极性二值序列，其长度为N，即

$$\boldsymbol{m}=\{m_i \mid m_i \in \{-1,1\}, 0 \leqslant i \leqslant N-1\} \tag{2-23}$$

该序列以较大的片率cr(大于1的正整数)进行扩展，得到长度为$N\cdot \mathrm{cr}$的扩展序列。这里，扩展方法有三种：第一种是按位扩展[60~63,68~70,154,198]，第二种是像铺瓷砖一样将原始信息序列延拓[113,195]，第三种是基于某个密钥K_1的随机扩展[174]。比较多见的是第一种，如图2-11(a)所示(cr=4)，其表达式为

$$\boldsymbol{s}=\{s_j \mid s_j=m_j, i\mathrm{cr} \leqslant j \leqslant (i+1)\mathrm{cr}-1, 0 \leqslant i \leqslant N-1\} \tag{2-24}$$

或写成[65]

$$\boldsymbol{s}=\{s_j \mid s_j=m_i, i=[j/\mathrm{cr}], 0 \leqslant j \leqslant N\cdot \mathrm{cr}-1\} \tag{2-25}$$

其中，中括号表示取整。第二种就是将原始信息互不重叠的周期延拓，如图2-11(b)所示(假设原始信息只有6位，cr=4)，只需要将上式的取整运算改为取模运算(求余数)即可，表达式如下：

$$\boldsymbol{s}=\{s_j \mid s_j=m_i, i=j \bmod (\mathrm{cr}), 0 \leqslant j \leqslant N\cdot \mathrm{cr}-1\} \tag{2-26}$$

第三种扩展方式先将$N\cdot \mathrm{cr}$个扩展位置根据密钥K_1随机分成N个非空子集$\mathbf{T}_i$(通常平均分)，也就是说将0,1,2,…,$N\cdot \mathrm{cr}-1$这$N\cdot \mathrm{cr}$个数，划分到N个子集中，满足：

3.2 DCT 变换域数字水印嵌入技术

上一节介绍的时空域数字水印嵌入方法的普遍缺点是：①嵌入的信息量不能太多；②鲁棒性差，尤其对滤波、量化和压缩攻击。为此，近年来的水印文献大都集中在变换域或频域，主要通过修改载体的变换域系数来实现水印嵌入过程。在变换域水印算法中，数字载体首先进行一种特定的正交变换，该变换可以针对整个载体（如整幅图像）或者载体的各部分（比如对图像进行分块，块大小一般为 8×8 或者 16×16）。嵌入空间是载体的某个频带或某些频带，这些频带对应的变换系数遵循一定的规则被修改、替换或交换。载体的低频信息反映了载体的主要轮廓，不应有较大的失真，水印的嵌入将影响不可见性；而载体的高频信息是人类感知系统不敏感的信息，通常被压缩技术所剔除，故在该频带嵌入水印，水印的鲁棒性较差。基于此，为了同时满足鲁棒性和不可见性，人们主张将水印嵌入到载体的中频系数中。

变换域水印嵌入算法的主要优点是：物理意义清晰；可充分利用人类的感知特性；不可见性和鲁棒性好；与压缩标准兼容。从本节开始的随后四节将介绍文献中已有的各种变换域数字水印技术，主要包括离散余弦变换（DCT）域、离散小波变换（DWT）域、离散傅里叶变换（DFT）域、离散分数傅里叶变换域、哈德码变换域、Fresnel 变换域、矢量变换域、KLT 变换域、Gabor 变换域、Zernike 变换域等。其中，DCT 域、DWT 域和 DFT 域比较常见，故对它们单独详细介绍。下面的每一节都先引出各种变换的定义，然后介绍各种嵌入方法，着重强调原理，限于篇幅不给出仿真实验结果。

离散余弦变换（discrete cosine transform，DCT）是数字信号处理技术中最常用的线性变换之一，和离散傅里叶变换一样，也存在着快速算法。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，因此它在数字音频信号压缩和图像压缩等领域得到广泛应用。特别地，数字图像的 JPEG 压缩标准就是建立在离散余弦变换基础上的。基于 JPEG 压缩标准模型的水印嵌入算法可以增强水印抵抗 JPEG 压缩的能力，因此离散余

弦变换在数字水印处理技术中受到了普遍重视。本节首先介绍离散余弦变换的定义，然后介绍基于离散余弦变换的各种水印嵌入算法。

3.2.1 离散余弦变换的定义和说明

1. 一维离散余弦变换的定义

为了统一描述，一维有限长离散序列 $x(i),0\leqslant i\leqslant N-1$ 用 $\boldsymbol{x}=\{x_i,0\leqslant i\leqslant N-1\}$ 或矢量 $\boldsymbol{x}=(x_0,x_1,\cdots,x_{N-1})^{\mathrm{T}}$ 来描述。二维有限长离散序列 $x(i,k),0\leqslant i\leqslant N_1-1,0\leqslant k\leqslant N_2-1$ 则用 $\boldsymbol{x}=\{x_{ik},0\leqslant i\leqslant N_1-1,0\leqslant k\leqslant N_2-1\}$ 或矩阵 $\boldsymbol{x}=\{x_{ik}\}_{N_1\times N_2}$ 表示。三维有限长离散序列 $x(i,k,l),0\leqslant i\leqslant N_1-1,0\leqslant k\leqslant N_2-1,0\leqslant l\leqslant N_3-1$ 则用 $\boldsymbol{x}=\{x_{ikl},0\leqslant i\leqslant N_1-1,0\leqslant k\leqslant N_2-1,0\leqslant l\leqslant N_3-1\}$ 或矩阵 $\boldsymbol{x}=\{x_{ikl}\}_{N_1\times N_2\times N_3}$ 表示。$\boldsymbol{x}$ 的一维离散余弦变换（1D-DCT）$\boldsymbol{X}=\{X_u,0\leqslant u\leqslant N-1\}$ 定义为

$$X_u=\alpha_u\sum_{i=0}^{N-1}x_i\cos\left[\frac{(2i+1)u\pi}{2N}\right] \tag{3-85}$$

相应的逆变换（1D-IDCT）定义为

$$x_i=\sum_{u=0}^{N-1}\alpha_u X_u\cos\left[\frac{(2i+1)u\pi}{2N}\right] \tag{3-86}$$

其中系数 α_u 定义为

$$\alpha_u=\begin{cases}\sqrt{1/N} & u=0\\ \sqrt{2/N} & u=1,2,\cdots,N-1\end{cases} \tag{3-87}$$

2. 二维离散余弦变换的定义

$\boldsymbol{x}$ 的二维离散余弦变换（2D-DCT）$\boldsymbol{X}=\{X_{uv},0\leqslant u\leqslant N-1,0\leqslant v\leqslant N-1\}$ 定义为

$$X_{uv}=\alpha_u\alpha_v\sum_{i=0}^{N-1}\sum_{k=0}^{N-1}x_{ik}\cos\left[\frac{(2i+1)u\pi}{2N}\right]\cos\left[\frac{(2k+1)v\pi}{2N}\right] \tag{3-88}$$

相应的逆变换（2D-IDCT）定义为

$$x_{ik}=\sum_{u=0}^{N-1}\sum_{v=0}^{N-1}\alpha_u\alpha_v X_{uv}\cos\left[\frac{(2i+1)u\pi}{2N}\right]\cos\left[\frac{(2k+1)v\pi}{2N}\right] \tag{3-89}$$

式（3-88）中系数 α_u,α_v 的定义与式（3-87）相同。

二维离散余弦变换不但能够将自然图像的主要信息集中到最少的低频系数上，而且引起的图像块效应最小，能够实现信息集中能力和计算复杂性的良好折中，因此它在压缩编码中得到广泛的应用。特别地，在二维离散余弦变换基础上建立了数字图像的 JPEG 有损压缩标准。在该标准的基本模型中，数字图像首先被分割成 8×8 的子块，然后经过基块离散余弦变换、系数量化和熵编码等过程最终实现了图像的有损压缩，具体介绍见后面的 JPEG 压缩域水印。离散余弦变换的实变换特性、良好的能量压缩能力和解相关能力、可以通过快速算法计算等优点使得它在数字水印嵌入算法的研究中具有很强的吸引力。

3.2.3 基于量化的嵌入方式

在时空域嵌入技术中曾提到，为实现盲抽取，一类在水印嵌入中常用的有效方法是量化索引调制(QIM)方法[44]。其中，比较著名的是抖动调制(dither modulation)方法[105]，其主要思想是根据水印位来调制量化区间。对于变换域来说，抖动调制的对象是变换域系数的幅度或相位，也可以是实部或虚部。下面首先介绍基本通用的单极性和双极性参数的抖动调制方法，然后给出文献中采用的各种 DCT 变换域抖动调制方法，最后给出其他一些特殊的量化方法。

假设待量化的参数为 f，量化步长为 Δ，待嵌入的水印比特为 $w\in\{0,1\}$，量化后得到的含水印系数为 f'。在嵌入水印比特 w 时，要根据 f 的取值范围(即极性的不同)选取不同的量化算法，分别介绍如下。

1. 单极性参数的抖动调制

单极性参数是指待量化参数的取值只能为正数或者负数(如离散傅里叶变换系数的幅度)。量化单极性参数 f 嵌入水印比特 w 的原理如图 3-28 所示，图 3-28(a)和图 3-28(b)分别为当 $f\geqslant 0$ 和 $f<0$ 时的情况。

单极性参数的量化过程及其表达式如下：

1) 划分区间集：选取量化步长 Δ 将坐标轴分割成如图 3-28 所示的 **A** 区间集和 **B** 区间集。

2) 确定坐标值的两重含义：如果用于计算，区间集内的坐标值具有表示数量大小的实际意义；如果用于表示水印比特信息，则无论坐标值大小，凡是属于 **A** 区间集的坐标都

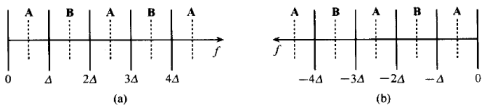

图 3-28　量化单极性参数嵌入水印信息

代表比特“1”，凡是属于 **B** 区间集的坐标都代表比特“0”。

3) 取整数商和余数运算：选取量化步长 Δ 对待量化参数 f 进行取整数商和余数运算。假设求得的整数商为 m、余数为 r，则有

$$m=\left[\frac{f}{\Delta}\right] \tag{3-101}$$

$$r=f-m\cdot\Delta \tag{3-102}$$

4) 量化参数：对参数 f 量化处理与水印比特 w 的取值密切相关：当 $w=1$ 时，使量化结果 f' 等于与 f 最接近的 **A** 区间集中某一区间的中间坐标值；当 $w=0$ 时，使 f' 等于与 f 最接近的 **B** 区间集中某一区间的中间坐标值。当 $f\geqslant 0$ 时，参数 f 的量化表达式如下(假设 $k=0,1,2,\cdots$)：

① 当 $m=0$ 且 $w=1$ 时：

$$f'=\frac{\Delta}{2} \tag{3-103}$$

② 当 $m=0$ 且 $w=0$ 时：

$$f'=\frac{3\Delta}{2} \tag{3-104}$$

③ 当 $m\neq 0$ 且 $w=1$ 时：

$$f'=\begin{cases}2k\Delta+\dfrac{1}{2}\Delta & \text{如 } m=2k\\ 2k\Delta+\dfrac{1}{2}\Delta & \text{如 } m=2k+1 \text{ and } r\leqslant\dfrac{1}{2}\Delta\\ 2k\Delta+2\Delta+\dfrac{1}{2}\Delta & \text{如 } m=2k+1 \text{ and } r>\dfrac{1}{2}\Delta\end{cases} \tag{3-105}$$

④ 当 $m\neq 0$ 且 $w=0$ 时：

$$f'=\begin{cases}(2k+1)\Delta+\dfrac{1}{2}\Delta & \text{如 } m=2k+1\\ 2k\Delta-\dfrac{1}{2}\Delta & \text{如 } m=2k \text{ and } r\leqslant\dfrac{1}{2}\Delta\\ (2k+1)\Delta+\dfrac{1}{2}\Delta & \text{如 } m=2k \text{ and } r>\dfrac{1}{2}\Delta\end{cases} \tag{3-106}$$

对单极性参数 f 进行量化操作后，水印比特 w 包含的信息由量化结果 f' 所在的区间集唯一确定：如果 f' 处在 **A** 区间集内，则 f' 代表水印比特信息“1”；反之，f' 处在 **B** 区间集内，则 f' 代表水印比特信息“0”。