图象工程（上）

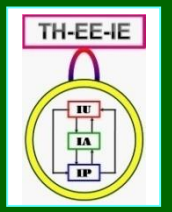
图 象 处 理

（第4版）

章毓晋

清华大学电子工程系 100084 北京

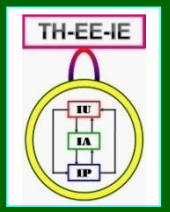
第4单元　拓展技术



- 第12章　图象信息安全
- 第13章　彩色图象处理
- 第14章　视频图象处理
- 第15章　多尺度图象处理

对图象的研究和应用一直是一个活跃的领域，新的理论、新的方法不断涌现，新的技术、新的手段也在不断拓展。基于前三个单元介绍的图象处理技术，进一步拓展

第12章　图象信息安全



(1)　如何控制和把握对特定图象的使用？

(2)　如何保护图象内容不被篡改伪造？

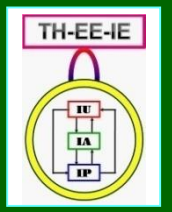
(3)　如何保护图象中的特定信息不被未允许的人发现和窃取？

(1)　图象水印技术：对知识产权的保护

(2)　图象认证和取证技术：对图象的完整性、来源、产生设备等进行鉴定

(3)　图象信息隐藏技术：实现秘密信息的传输

第12章　图象信息安全



12.1　水印原理和特性

12.2　DCT域图象水印

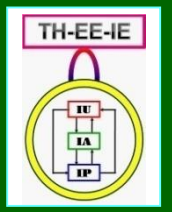
12.3　DWT域图象水印

12.4　水印性能评判

12.5　图象认证和取证

12.6　图象信息隐藏

12.1 水印原理和特性

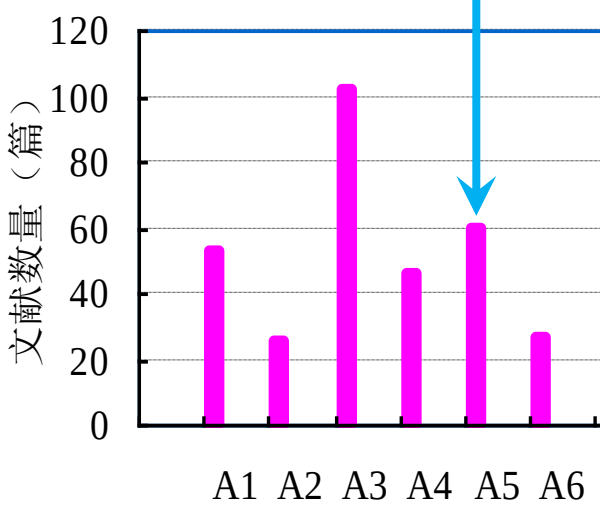


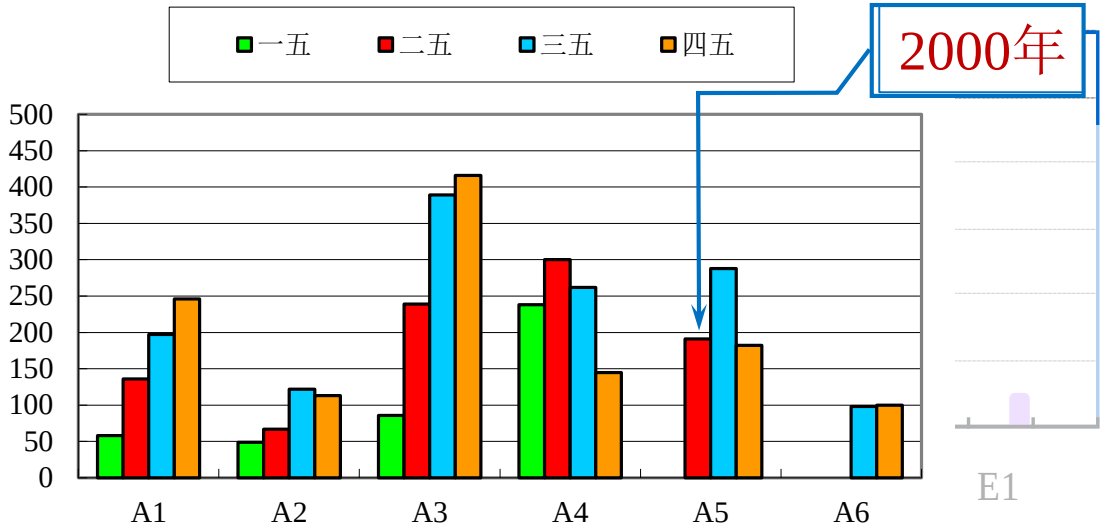
2002年《图象工程》第1版（附册）

2006年《图像工程》第2版（上册）

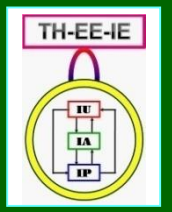
综述：中国图象工程——A：图象处理

A5：图象数字水印和图象信息隐藏





12.1 水印原理和特性



图象水印的主要用途包括

(1) **版权鉴定**：提供证明所有者的信息，从而保护图象产品的版权（著作权）

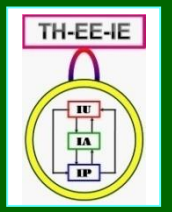
(2) **使用者鉴定**：可将合法用户的身份记录在水印中，并用来确定非法复制的来源

(3) **真实性确认**：水印的存在可以保证图象没有被修改过

(4) **自动追踪**：通过追踪水印，从而知道何时何地图象被使用，有利于版税征收

(5) **复制保护**：利用水印可以规范对图象的使用，如仅播放而不复制

12.1 水印原理和特性



对水印的操作主要是嵌入和检测（提取）

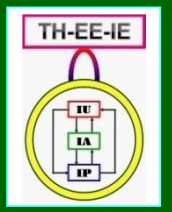
不同类型的水印有不同的特点

12.1.1 水印的嵌入和检测

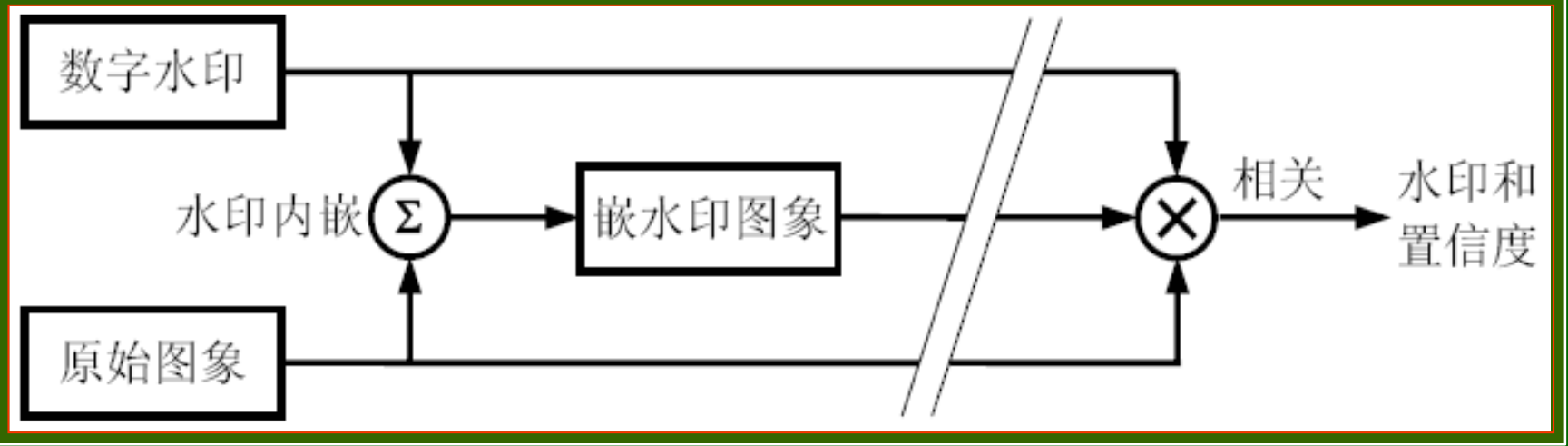
12.1.2 水印特性

12.1.3 水印分类

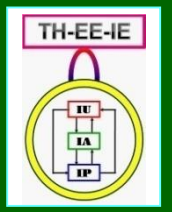
12.1.1 水印的嵌入和检测



- 利用水印保护数字产品需进行两个操作：
  - 水印的嵌入：在数字产品使用前将水印加入到数字产品中以进行保护
  - 水印的检测：将嵌入到数字产品中的水印提取出来以验证或表明版权



12.1.1 水印的嵌入和检测



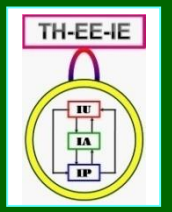
- 设原始图象为$f(x, y)$，水印为$W(x, y)$，嵌入水印的图象为$g(x, y)$
- 水印嵌入：　$g = E(f, W)$
- 给出待检测图象$h(x, y)$，抽取待验证的可能水印$w(x, y)$：　$w = D(f, h)$
- 考虑原始水印和可能水印的相关函数$C(.,.)$

如果（T为预先确定的阈值）：

$$C(W, w) > T$$

则认为水印存在，否则认为水印不存在

12.1.2 水印特性



1. **显著性**

⇒ 不可感知性或不易察觉性

一是水印不易被接收者或使用者察觉，二是水印的加入不影响原产品的视觉质量

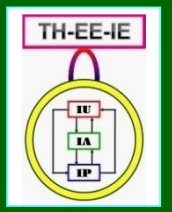
2. **稳健性**

抗攻击性或鲁棒性，抵御外界加工的能力

图象产生失真情况下，仍保证其自身完整性和对其检测的准确性

易损水印对外界处理有敏感的反应

12.1.3 水印分类



1. 公开性分类

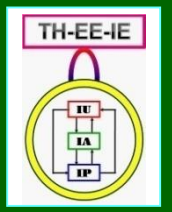
(1) **私有水印**：其检测需要提供原始数字产品，借此作为提示寻找水印的位置

(2) **半私有水印**：其检测不需用原始数字产品，但须回答是否有水印的问题

(3) **公有水印（盲水印）**：其检测既不要求保密的原始数字产品，又不要求嵌入水印后的数字产品

(4) **不对称水印（公钥水印）**：任何用户能看到但去不掉的水印

12.1.3 水印分类



2. 感知性分类

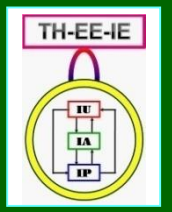
(1) 可感知的水印

- 如纸张内嵌的图案，电视屏幕上的台标
- 可证明数字产品的归属

(2) 不可感知的水印

- 隐藏在数字产品之中
- 用于检测非法复制，鉴别产品的真伪
- 不可见形式，防止被擦除或取代，应不影响原作品的观赏价值和使用价值

12.1.3 水印分类



3. 含义/内容分类

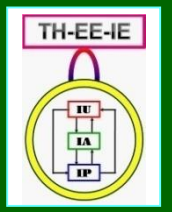
(1) 无意义水印

- 利用伪随机序列表达有无，难以伪造
- 无水印：H_0： $g - f = n$
- 有水印：H_1： $g - f = w + n$

(2) 有意义水印

- 本身有特定/确切含义（多比特信息）
- 文字串、图标、图象等，可提供的信息多，对其嵌入和检测的要求也高

12.1.3 水印分类



4. 变换域水印

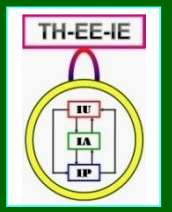
大多数图象水印的嵌入都是在变换域中（而不是在空域中）进行的。变换域法主要优点：

(1) 水印信号的能量可广泛分布到所有象素上，有利于保证不可见性

(2) 可以比较方便地结合人类视觉系统的某些特性，有利于提高稳健性

(3) 变换域方法与大多数图象编码国际标准兼容，可直接实现压缩域内的水印算法（此时的水印也称比特流水印），从而提高效率

12.2 DCT域图象水印

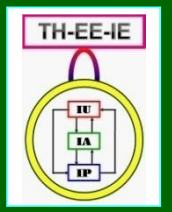


在DCT域中，利用AC系数可加强嵌入的秘密性，而利用DC系数可增加嵌入的数据量

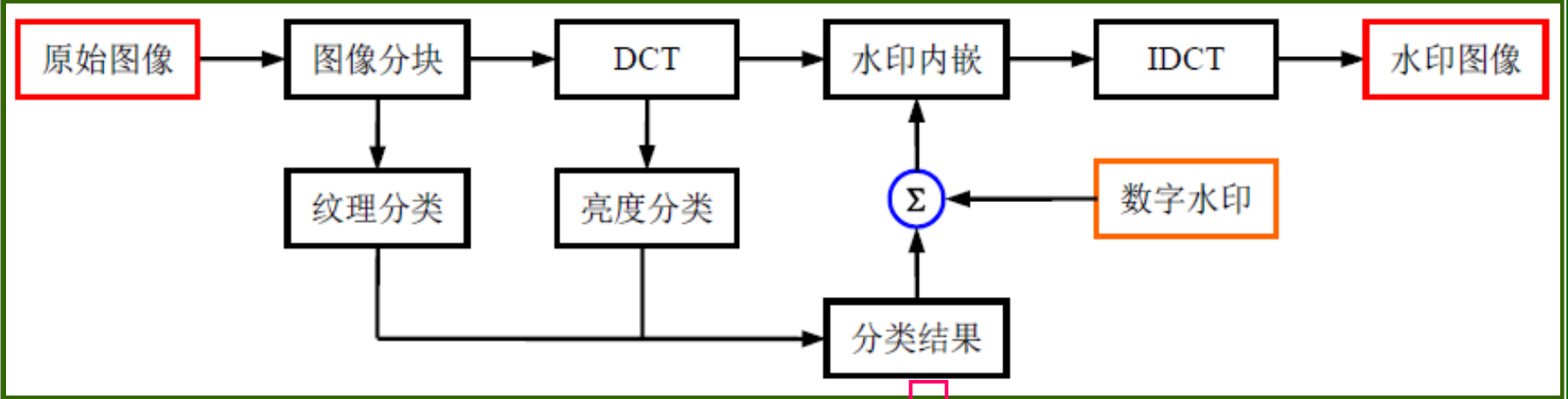
12.2.1 无意义水印算法

12.2.2 有意义水印算法

12.2.1 无意义水印算法

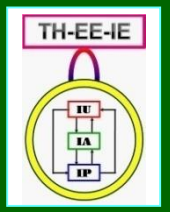


- 综合利用DC和AC系数的方案



- 将图象块分为三类：
  ① 具有低亮度且纹理简单的块（嵌入较少水印）
  ② 具有高亮度且纹理复杂的块（嵌入较多水印）
  ③ 其他块（嵌入量适中）

12.2.1 无意义水印算法



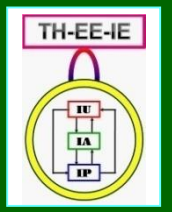
具体步骤/细节

- 产生一个服从高斯分布$N(0, 1)$的随机序列作为拟嵌入的水印$\{g_m: m = 0, 1, 2, \ldots, M-1\}$
- 选取4个DCT系数，即$F_i(0, 0)$，$F_i(0, 1)$，$F_i(1, 0)$和$F_i(1, 1)$
- 取随机序列长度为图象分块数的4倍
- 将随机序列乘以适合的拉伸因子后嵌入DCT系数

$$F_i'(u,v)=\begin{cases} F_i(u,v)\times(1+a\,g_m) & m=4i,\quad (u,v)=(0,0) \\ F_i(u,v)+b\,g_m & m=4i+2u+v,\quad (u,v)\in\{(0,1),(1,0),(1,1)\} \\ F_i(u,v) & \text{其他} \end{cases}$$

$2u+v$ → 1， 2， 3

12.2.1 无意义水印算法



- 水印的检测采用假设-相关检测方法

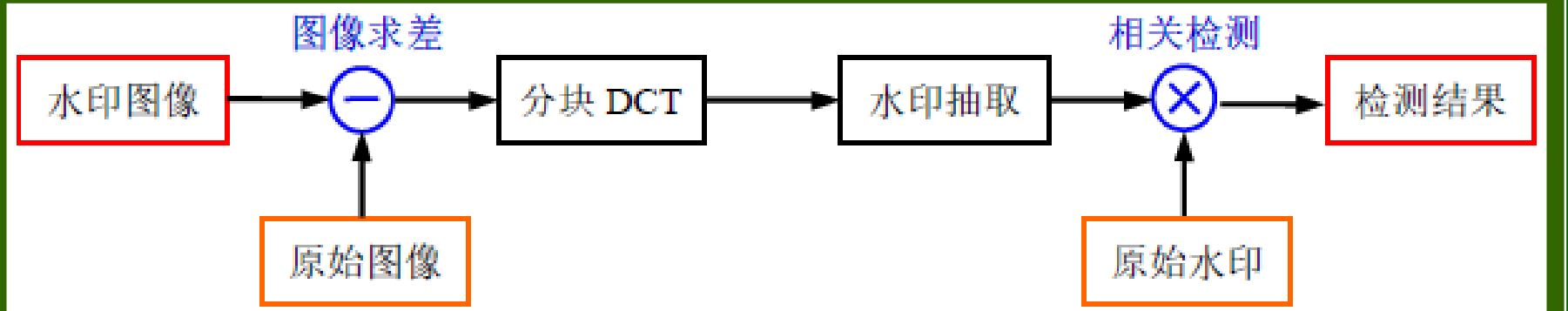


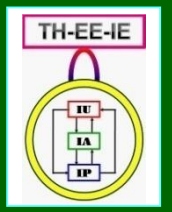
图 12.2.3 水印检测流程

具体步骤

(1) 计算原始图象$f(x, y)$和拟检测图象$h(x, y)$的差

$$e(x,y)=f(x,y)-h(x,y)=\bigcup_{i=0}^{I-1}e_i(x',y') \qquad 0\le x',y'<8$$

12.2.1 无意义水印算法



(2) 对差图象的每个块计算DCT

$$E_i(u',v')=\mathrm{DCT}\{e_i(x',y')\} \qquad 0\le x',y'<8$$

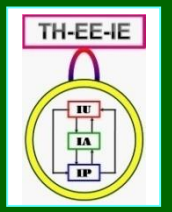
(3) 从图象块DCT提取可能的水印序列

$$w_i(u',v')=\{g_m,\ m=4i+2u'+v'\}=E_i(u',v')$$

(4) 计算可能的水印和原嵌入水印的相关性，并作出判断

$$C(W,w)=\frac{\sum_{j=0}^{4I-1}\left(w_j\bullet g_j\right)}{\sqrt{\sum_{j=0}^{4I-1}w_j^2}}>T$$

12.2.2 有意义水印算法



- 对上述无意义水印方案进行改进，可得到用于有意义水印的算法

(1) 构造符号集（有意义符号，L个）

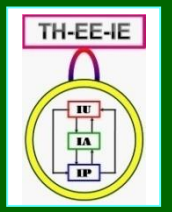
(2) 将每个符号对应一个二值序列（长度M）

(3) 让序列中“0”和“1”的出现服从Bernoulli分布（保证随机性）

(4) 将序列扩展成（符号数L的）整倍数

(5) 将扩展序列加到DCT块的系数中

12.2.2 有意义水印算法



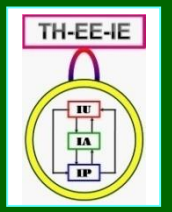
- ✓ 对有意义水印检测的前3个具体步骤与对无意义水印的检测相同{P.276}
- ✓ 在(4)中，设第i次提取时，w_i^*是提取出的信号强度；w_i^k是第k个匹配滤波器的输出，它们之间的相关为

$$C_k(w^*, w^k) = \frac{\sum_{i=0}^{M-1}(w_i^* \bullet w_i^k)}{\sqrt{\sum_{i=0}^{M-1}(w_i^*)^2}}$$

- ✓ 寻找 j（$1 \le j \le L$）

$$C_j(w^*, w^j) = \max\left[C_k(w^*, w^k)\right] \quad 1 \le k \le L$$

12.3 DWT域图象水印

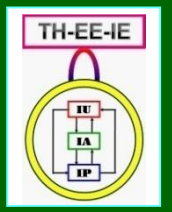


{优点源自小波变换（10.4节）的特性}

12.3.1 人眼视觉特性

12.3.2 小波水印算法

12.3.1 人眼视觉特性



掩盖特性和视觉阈值

(1) 人眼对不同方向不同层次的高频子带图象的噪声不太敏感，另外对45°方向的子带（如HH子带）图象的噪声也不太敏感

掩盖因子：$M(l, d)$

层数

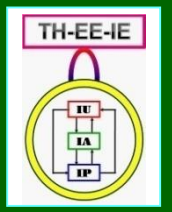
方向

$$M(l,d)=M_l\times M_d$$

$$M_d=\begin{cases}\sqrt{2} & d\in \mathrm{HH}\\ 1 & \text{其他}\end{cases}$$

$$M_l=\begin{cases}1 & l=0\\ 0.32 & l=1\\ 0.16 & l=2\\ 0.1 & l=3\end{cases}$$

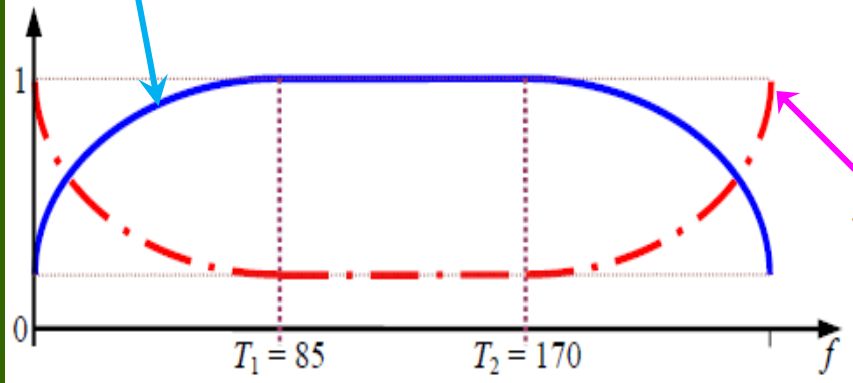
12.3.1 人眼视觉特性



掩盖特性和视觉阈值

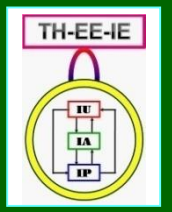
(2) 人眼对不同亮度区域噪声的视觉敏感性不同，通常对中等灰度最为敏感，而趋向低灰度和高灰度两个方向时敏感度都会非线性下降

掩盖因子：$B(u, v)$，图象块均值为m



$$B(u,v)=\begin{cases}\dfrac{(0.2-0.02)[m-T_1]^2}{T_1^2}+0.02 & m\le T_1\\ 0.02 & T_1<m\le T_2\\ \dfrac{(0.2-0.02)[m-T_2]^2}{(255-T_2)^2}+0.02 & m>T_2\end{cases}$$

12.3.1 人眼视觉特性



掩盖特性和视觉阈值

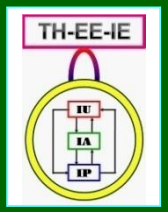
(3) 人眼对图象平滑区的噪声较为敏感而对纹理区的噪声较不敏感。可根据图象分块区域的熵值来计算纹理掩盖效应

掩盖因子：$H(u,v)$，图象块的熵值为H

$$H(u,v)=k\frac{H-\min(H)}{\max(H)-\min(H)}$$

综合 $$T(u,v,l,d)=M(l,d)B(u,v)H(u,v)$$

12.3.2 小波水印算法



1. 水印嵌入（仅讨论无意义水印）

- 选用具有高斯分布$N(0, 1)$，长度为M的实数随机序列作为水印W，即$W = \{w_1, w_2, \ldots, w_M\}$
- 基本嵌入流程与在DCT域中类似

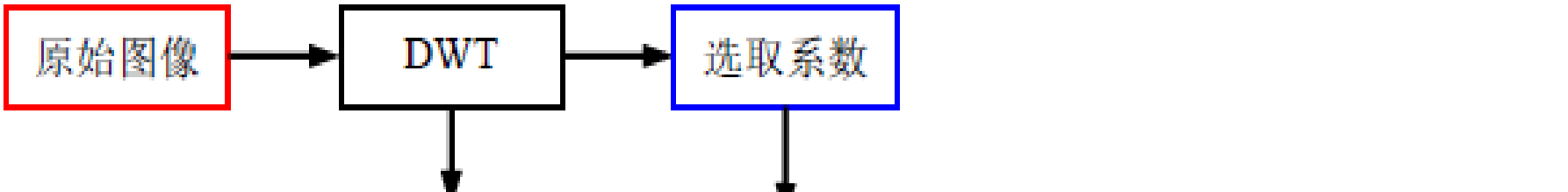
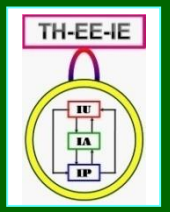


图 12.3.2 小波域水印嵌入流程

12.3.2 小波水印算法



1. 水印嵌入

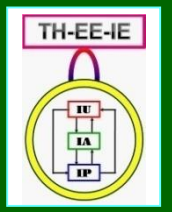
(1) 小波变换，分别得到一个逼近子图（最低频子带）和3L个细节子图（含高频子带）

(2) 计算高频子图象内的人眼视觉掩盖特性的视觉阈值$T(u, v, l, d)$，并选择小波系数插入水印

(3) 嵌入水印（即用水印序列来调制前N个小波系数） $F'(u,v) = F(u,v) + qw_i$

(4) 将嵌入水印的高频子图象结合低频子图象一起进行小波反变换，得到嵌水印图象$f'(x, y)$

12.3.2 小波水印算法



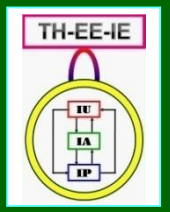
2. 水印检测

- 对原始图象f和待测图象f''（有可能与原嵌入水印图象f'不同）都进行L级小波分解，得到各自的1个最低频子带和$3L$个高频子带
- 根据密钥，获得重要系数集，比较系数值，提取出待测水印序列$W'' = \{w_1', w_2', \ldots, w_M'\}$
- 计算

$$C_N(W,W'') = \frac{\sum_{i=1}^{L}(w_i - W_m)(w''_i - W''_m)}{\sqrt{\sum_{i=1}^{L}(w_i - W_m)^2}\sqrt{\sum_{i=1}^{L}(w''_i - W''_m)^2}}$$

（归一化相关系数）

12.4 水印性能评判



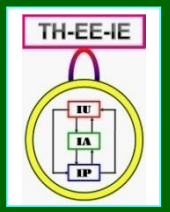
对水印性能的检测和评价与所关心的水印特性和指标密切相关

12.4.1 失真测度

12.4.2 基准测量和攻击

12.4.3 水印性能测试示例

12.4.2 基准测量和攻击

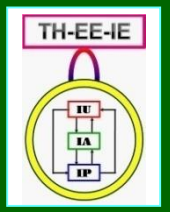


1. 基准测量方法

基准测量（benchmarking）

- 先确定一定的图象/视频数据
- 嵌入尽可能多但还不至于导致非常影响视觉质量（根据某种测度）的水印
- 对嵌入水印的数据进行处理或攻击
- 通过测量所产生误差的比例来估计水印方法的（抗处理或攻击）性能

12.4.2 基准测量和攻击



2. 攻击类型

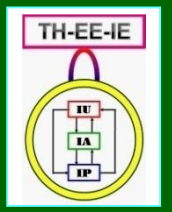
对水印的攻击是未经授权的操作

（1）**检测**：例如一个水印产品的使用者检测了本应由所有者才检测的水印，这也称**被动攻击**

（2）**嵌入**：例如一个水印产品的使用者对产品嵌入了一个本应由所有者才能嵌入的水印，这也称**伪造攻击**

（3）**删除**：例如一个水印产品的使用者删除了本应由所有者才有权删除的水印（**删除攻击**）

12.5 图象认证和取证



12.5.1 基本概念

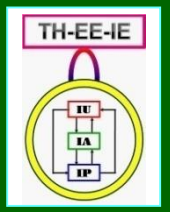
12.5.2 图象被动取证

12.5.3 图象可逆认证

12.5.4 图象取证示例

12.5.5 图象反取证

12.5.1 基本概念



1. 图象篡改

对图象内容未经所有者允许的修改（版权、完整性、原始性等），真实性篡改：

(1) 合成：借助复制-粘贴操作

(2) 增强：弱化或突出某些细节

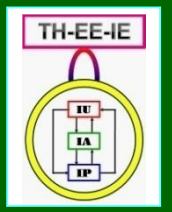
(3) 修整：对一些局部区域进行空间调整

(4) 变形：将源图象渐变演变成目标图象

(5) 计算机生成：生成新的非/真实感图象

(6) 绘画：用图象处理软件进行图象制作

12.5.1 基本概念



2. 图象认证

确定图象的身份，鉴别图象的来源

对图象真实性的鉴别要考虑场景的属性，特别是一致性（篡改局部）

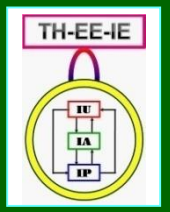
对图象来源的鉴别要考虑图象获取设备和显示设备（考虑设备的内在特征）

根据图象认证的目的，认证还可以分为：

完整性认证：关注图象内容的表述形式

鲁棒性认证：关注图象内容的表达结果

12.5.1 基本概念



3. 图象取证

对源于图象的证据进行确定、收集、识别、分析，以及出示法庭的过程

图象取证的方法：主动、半主动、被动

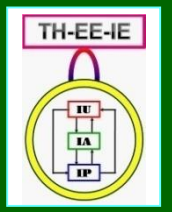
图象取证的类型：

(1) 图象真实性取证：防伪检测

(2) 图象来源取证：判断获取或输出设备

(3) 图象隐写取证：判断图象中是否嵌入了秘密信息，并提取出秘密信息

12.5.2 图象被动取证



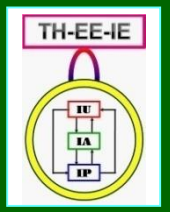
图象盲取证（不利用预先操作）

(1) 图象来源认证：不同的电子设备具有不同的物理特征，其生成的数字图象也具有相互不同的数字特征

(2) 图象篡改检测：复制-粘贴操作、模糊润饰操作和篡改之后的重新存储操作等，这些操作都将改变数字图象的统计特征

(3) 图象隐秘分析：图象中是否嵌入了秘密信息、嵌入在什么位置，嵌入量有多大等

12.5.3 图象可逆认证



要求认证过后，必须对原始图象进行无损还原/完全恢复，即认证过程需要可逆（无损检测）

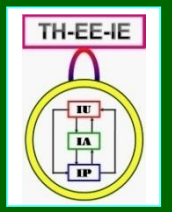
可逆认证（借助脆弱水印技术）

(1) 基于数据压缩的可逆水印：向原始图象中嵌入恢复信息，以完全恢复出原始图象

(2) 基于差数扩展的可逆水印：将水印嵌入到一些象素值的最不重要位面（LSB）上，然后用这些修改后的象素值重构图象

(3) 基于直方图修改的可逆水印：选择图象直方图中若干个最大点和最小点进行信息隐藏

12.5.4 图象取证示例



根据打印的文档、对打印机进行鉴别取证

将纸质打印文档扫描为图象，通过对图象提取特征，区分用不同打印机打印出的文档

实验：打印了同一本英文书籍的70页

以1200 dpi的分辨率扫描

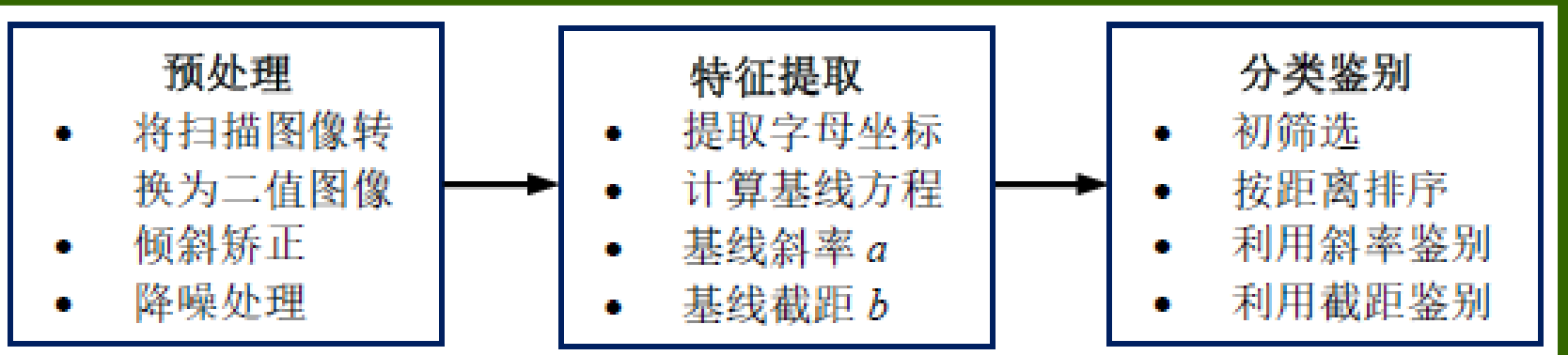
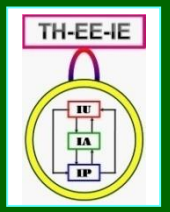


图 12.5.1 打印机鉴别取证流程图

12.5.5 图象反取证

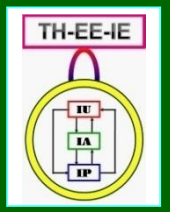


图象取证和图象反取证之间的关系相当于矛和盾的关系

图象取证的基本依据是：图象的成象过程或者处理过程都会留下特殊的痕迹，而取证技术通过识别待取证图象中是否存在相应痕迹而判定其原始性和真伪

图象反取证就是试图运用相应的后处理操作来消除或掩盖篡改的遗留痕迹，使与之对应的取证技术的检测性能大大下降或失效

12.6 图象信息隐藏

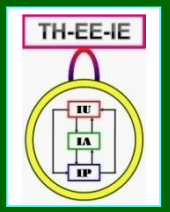


一个比较广泛的概念，一般指将某些特定的信息有意地和隐蔽地嵌入某种载体，以达到某种保密或保护信息的目的

12.6.1 信息隐藏技术分类

12.6.2 基于迭代混合的图象隐藏

12.6.1 信息隐藏技术分类



根据是否对特定信息本身存在性的保密或不保密，信息隐藏可以是隐秘的或非隐秘的

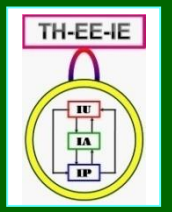
根据这些特定信息与载体相关或不相关，信息隐藏又可分为水印类型的或非水印类型的

表 12.6.1 信息隐藏技术分类

	与载体相关	与载体不相关
隐藏信息存在性	(1) 隐秘水印	(3) 秘密通信
已知信息存在性	(2) 非隐秘水印	(4) 秘密嵌入通信

被动认证 vs. 主动水印 非水印

12.6.2 基于迭代混合的图象隐藏



1. 图象混合

$$b(x,y)=\alpha f(x,y)+(1-\alpha)s(x,y)$$

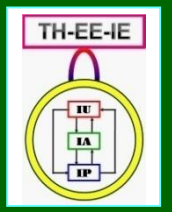
参数α为0或1时称为平凡混合

载体图象f　　隐藏图象s　　混合图象b

(a)　(b)　(c)

图 12.6.1　图像混合示例

12.6.2 基于迭代混合的图象隐藏



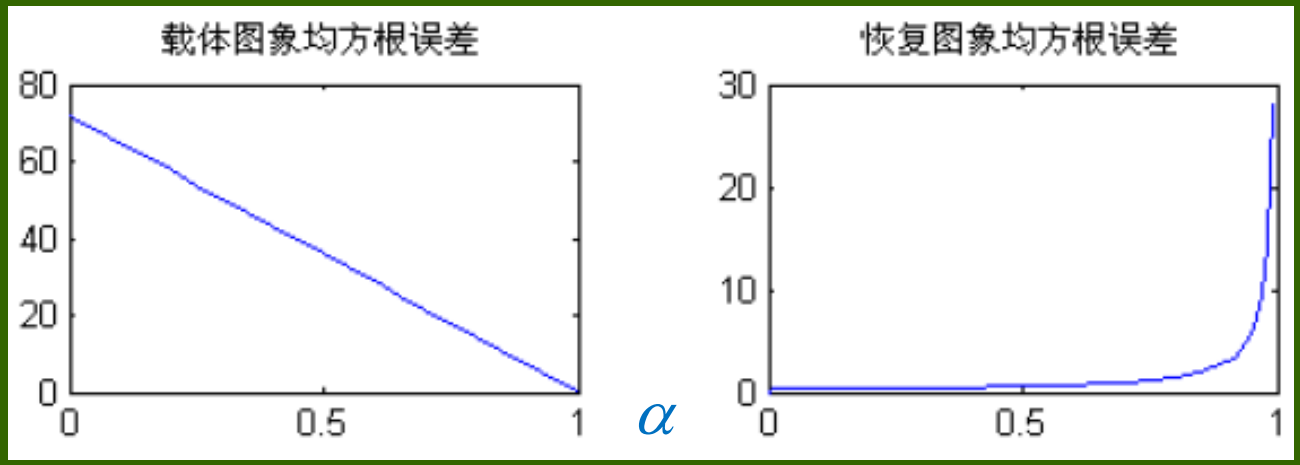
1. 图象混合

当混合参数α接近1时，混合图象$b(x, y)$就接近于图象$f(x, y)$；当混合参数α接近0时，混合图象$b(x, y)$就接近于图象$s(x, y)$

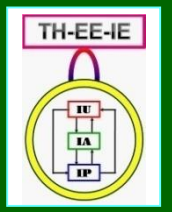
隐藏图象恢复公式：

$$s(x,y)=\frac{b(x,y)-\alpha f(x,y)}{1-\alpha}$$

取整误差



12.6.2 基于迭代混合的图象隐藏



1. 图象混合

混合参数越接近1，图象隐藏的效果就越好，而恢复图象的质量就越差。反之，如果要求恢复的图象效果好，则混合参数就不能太接近1

存在最佳的混合隐藏，即能使混合图象与恢复图象误差之和最小的图象混合

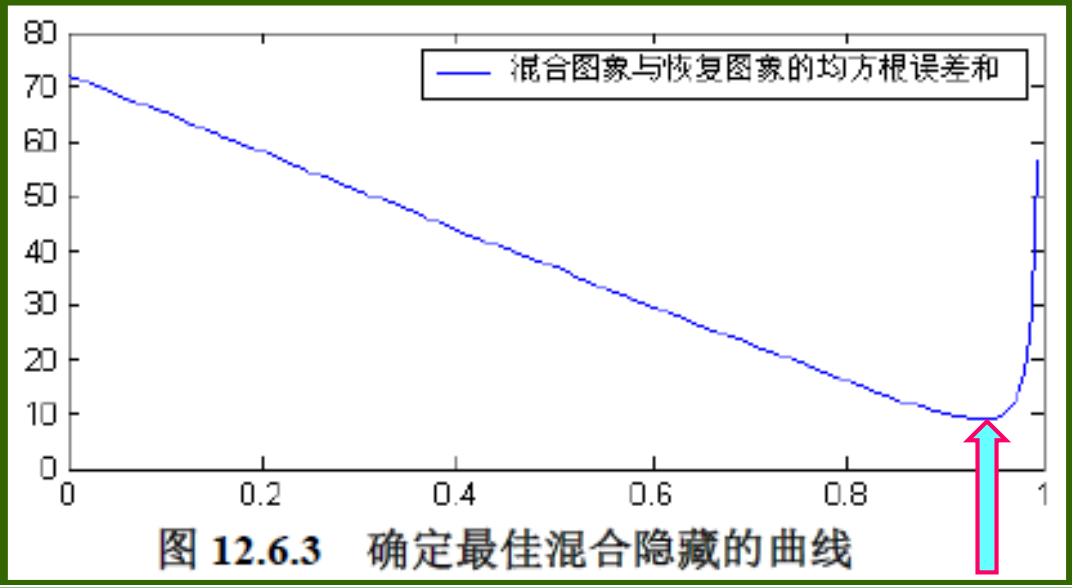
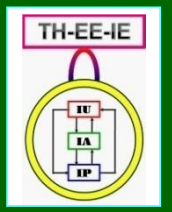


图 12.6.3 确定最佳混合隐藏的曲线

12.6.2 基于迭代混合的图象隐藏



2. 图象的单幅迭代混合

设$\{\alpha_i \mid 0 \leqslant \alpha_i \leqslant 1, i = 1, 2, \ldots, N\}$为$N$个实数

- 对图象$f(x, y)$和$s(x, y)$进行α_1混合得

$$b_1(x, y) = \alpha_1 f(x, y) + (1 - \alpha_1)s(x, y)$$

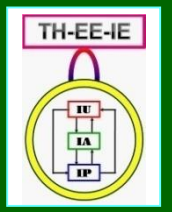
- 对图象$f(x, y)$和$b_1(x, y)$进行α_2混合得

$$b_2(x, y) = \alpha_2 f(x, y) + (1 - \alpha_2)b_1(x, y)$$

- 依次进行混合可得

$$b_N(x, y) = \alpha_N f(x, y) + (1 - \alpha_N)b_{N-1}(x, y)$$

12.6.2 基于迭代混合的图象隐藏



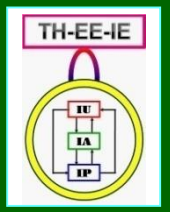
3. 图象的多幅迭代混合

单幅迭代混合算法将一幅秘密图象隐藏在一幅载体图象中

如果攻击者截获了载体图象和混合图象并产生了怀疑，则攻击者借助原始载体图象就有可能通过相减恢复出秘密图象

设 $f_i(x, y)$ $(i=1, 2, \ldots, N)$ 为一组载体图象，$s(x, y)$为一幅隐藏图象，$\{\alpha_i \mid 0 \leqslant \alpha_i \leqslant 1, i = 1, 2, \ldots, N\}$ 为给定的N个实数

12.6.2 基于迭代混合的图象隐藏



3. 图象的多幅迭代混合

对图象$f_1(x, y)$和$s(x, y)$进行α_1混合得

$$b_1(x, y)=\alpha_1 f_1(x, y)+(1-\alpha_1)s(x, y)$$

对图象$f_2(x, y)$和$b_1(x, y)$进行α_2混合得

$$b_2(x, y)=\alpha_2 f_2(x, y)+(1-\alpha_2)b_1(x, y)$$

依次进行混合可得

$$b_N(x,y)=\alpha_N f_N(x,y)+(1-\alpha_N)b_{N-1}(x,y)$$

图象$b_N(x, y)$称为图象$f(x, y)$和$s(x, y)$关于α_i和$f_i(x, y)$（$i=1, 2, \ldots, N$）的N重迭代混合图象

联　系　信　息

- 通信地址：北京清华大学电子工程系
- 邮政编码：100084
- 办公地址：清华大学，罗姆楼，6层305室
- 办公电话：(010) 62798540
- 传真号码：(010) 62770317
- 电子邮件：zhang-yj@tsinghua.edu.cn
- 个人主页：oa.ee.tsinghua.edu.cn/~zhangyujin/