数字媒体技术基础
——多媒体数据安全

王晗

wanghan@bjfu.edu.cn

专题提纲

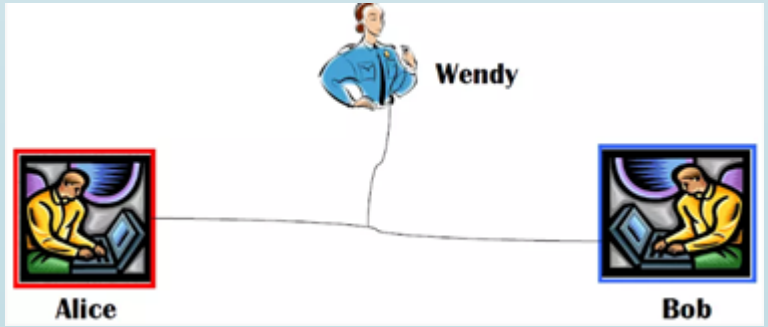
- 多媒体数据安全
- 多媒体数据的信息隐藏
- 基于图像的信息隐藏
- 基于视频的信息隐藏
- 基于音频的信息隐藏

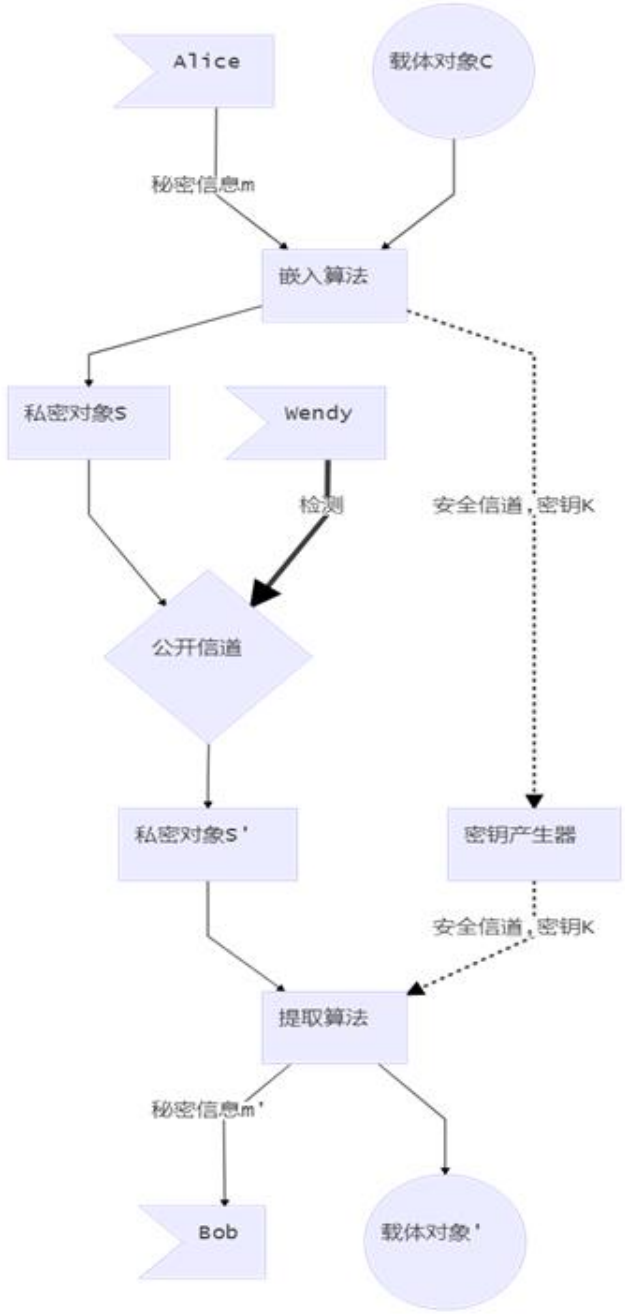
多媒体数据安全

- 隐写术(Steganography)
- 数字水印(Digital Watermarking)
- 多媒体取证(Multimedia Forensics)
- 多媒体感知哈希(Perceptual Hash)
- 多媒体内容隐私(Multimedia Privact)

隐写术(Steganography)

- 隐写术（Steganography）将信息嵌入媒体数据中进行传送。
- 隐写术的基本思想是把秘密消息嵌入在正常的媒体数据中，通过隐藏消息的存在行来构建隐蔽通信。
- 对于多媒体数据隐写术的研究主要以对抗式研究展开：信息隐藏与信息隐藏分析。
- demo





数字水印(Digital Watermarking)

- 将一些标识信息（即数字水印）直接嵌入数字载体当中（包括多媒体、文档、软件等）或是间接表示（修改特定区域的结构），且不影响原载体的使用价值，也不容易被探知和再次修改。但可以被生产方识别和辨认。通过这些隐藏在载体中的信息，可以达到确认内容创建者、购买者、传送隐秘信息或者判断载体是否被篡改等目的。数字水印是保护信息安全、实现防伪溯源、版权保护的有效办法，是信息隐藏技术研究领域的重要分支和研究方向。

多媒体取证(Multimedia Forensics)

- 对多媒体原始性进行鉴别
- 对多媒体内容的无损取证溯源技术主要可以分类两大类：一是对多媒体内容进行篡改伪造取证；二是对多媒体的获取设备进行溯源分析。

DeepFakes and Beyond: A Survey of Face Manipulation and Fake Detection

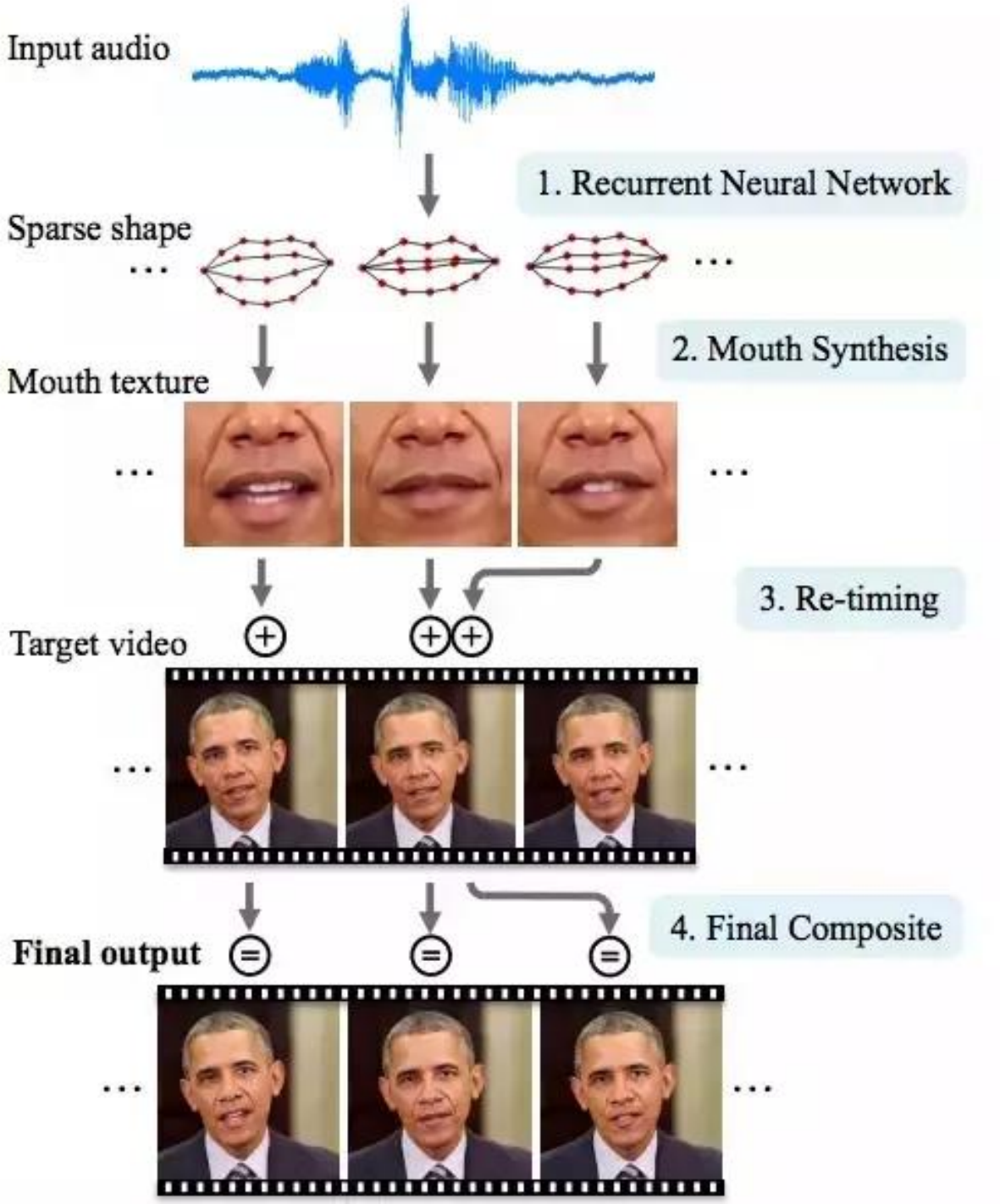
Ruben Tolosana, Ruben Vera-Rodriguez, Julian Fierrez, Aythami Morales and Javier Ortega-Garcia
Biometrics and Data Pattern Analytics - BiDA Lab, Universidad Autonoma de Madrid, Spain
ga}@uam.es

Output Obama Video

Deepfake


hua_jiang:85.6%
die_yu:78.9%
hua_jiang:85.3%
bilibili 首发
@Jack-Cui
Lv.60
9319 / 9319
×287

人脸属性操纵


Input audio
1. Recurrent Neural Network
Sparse shape
2. Mouth Synthesis
Mouth texture
3. Re-timing
Target video
4. Final Composite
Final output

多媒体感知哈希(Perceptual Hash)

- 感知哈希是一系列哈希算法的总称。通过将多媒体数据集映射至一个感知特征集。在这个特征集中，每一条多媒体数据都有一个属于自身的唯一“指纹”数据，这些指纹可以进行相互比较。在这个感知特征集中越相似的图像“指纹”越相似。

感知哈希pHash

感知哈希算法可以获得更精确的结果，它采用的是DCT（离散余弦变换）来降低频率。

a) 缩小尺寸

为了简化了DCT的计算，pHash以小图片开始（建议图片大于8x8，32x32）。

b) 简化色彩

将图片转化成灰度图像，进一步简化计算量（把缩放后的图片转化为256阶的灰度图，灰度转换基础的心理学公式：Gray = R0.299 + G0.587 + B0.114）。

c) 计算DCT

DCT是把图片分解频率聚集和梯状形。这里以32x32的图片为例

d) 缩小DCT

DCT的结果为32x32大小的矩阵，但只需保留左上角的8x8的矩阵，这部分呈现了图片中的最低频率。

e) 计算平均值

计算DCT的均值

f) 进一步减小DCT

根据8x8的DCT矩阵进行比较，大于等于DCT均值的设为”1”，小于DCT均值的设为“0”。图片的整体结构保持不变的情况下，hash结果值不变。

g) 构造hash值

组合64个bit位生成hash值，顺序随意但前后保持一致性即可。

h）对比指纹：计算两幅图片的指纹，计算汉明距离。

多媒体内容隐私(Multimedia Privact)

- 对多媒体敏感内容保护进行保护
- 目前主流社交媒体中对于图像分享所提供的的隐私保护仅仅是面向大众的基础性保护，如允许用户自行设定图像的可见范围以及有效期等，属于访问权限控制。一些技术提出将照片中小部分重要信息和其余部分格式分别编码存储，以实现隐私保护。
- 对于视频的隐私保护主要针对数据源的保护及编码过程结合的保护，目的是重点保护隐私区域，同时不影响视频的正常使用。视频中隐私保护的目标主要是人脸或身体等有可能泄露用户身份的部分。其中使用到的技术主要是人脸检测技术，直接对人脸进行识别，还有利用辅助信息自适应低根据需求选取隐私区域。

315晚会曝光人脸识别摄像头

个人信息保护的主要规则

- 当前我国个人信息保护的规则仍以“知情-同意”作为个人数据收集和使用的基本条件，以个人信息安全和国家安全作为个人信息保护的主要目标

个人信息保护具体规则

收集使用	存储、管理	向他人提供	跨境流动
• 应遵循合法、正当、必要的原则 • 公开收集、使用规则 • 明示收集、使用信息的目的、方式和范围 • 经被收集者同意	• 不得泄露、篡改、毁损其收集的个人信息 • 采取技术措施和其他必要措施，确保其收集的个人信息安全	• 未经被收集者同意，不得向他人提供个人信息，匿名化除外 • 不得非法出售或者非法向他人提供个人信息	• 关键信息基础设施中的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当进行安全评估

法律责任

民事法律责任

✓ 网络用户、网络服务提供者利用网络侵害他人民事权益的，应当承担侵权责任。

行政法律责任

✓ 警告、没收违法所得、罚款、暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照

刑事法律责任

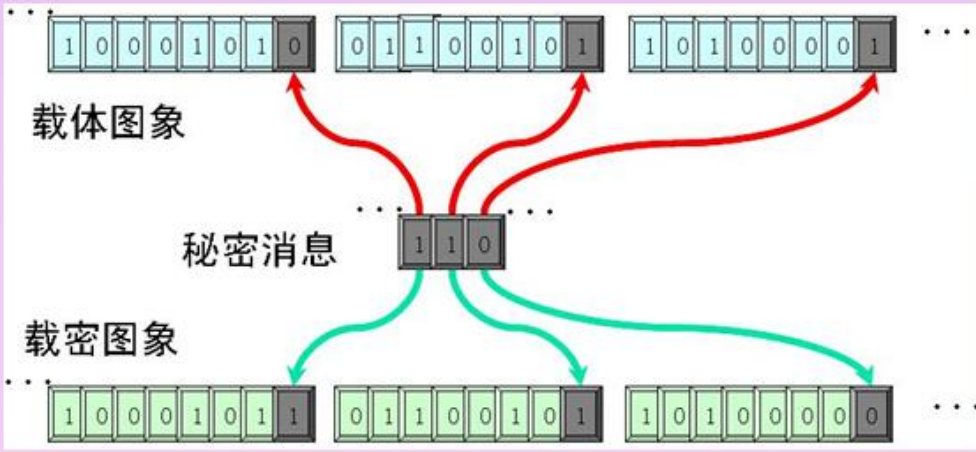
✓ 情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金

个人信息保护及法律责任

基于图像的信息隐藏（Information Hiding）

- 基于图像的信息隐藏充分利用人们“所见即所得”的习惯心理和视觉上的欺骗性，可以将秘密信息存放到对图像质量影响较小的“特殊位置”。由于加入的数据量相对于图像中的大量像素来说“微不足道”，因此从视觉上几乎无法察觉，在传输和公开的过程中，只有知道提取方法的人才能还原其中的秘密信息。
- 基于图像的信息隐藏一般应满足如下要求：
  - 隐蔽性
  - 鲁棒性
  - 安全性
  - 对称性
  - 可纠错性
  - 效率

基于图像的信息隐藏



秘密信息替换载体图像的LSB成为载密图像

在静止图像中的信息隐藏技术主要有如下4种：

- 基于空间域的隐藏技术

直接在图像原始像素中嵌入信息的方法，包括最低有效位（LSB）法，把待隐藏信息编码隐藏到宿主的颜色最低有效位上，可隐藏较大容量的信息。

- 基于变换域的隐藏技术

利用人眼对高频分量上噪声不敏感的特点，将带隐藏信息编码到图像的高频分量，以实现信息隐藏的目的，包括扩频隐藏、DCT隐藏、小波隐藏技术等

- 基于融合的隐藏技术

利用数字图像的自相关性，通过放大原始公开图像来隐藏与公开图像同样大小的数字图像。该方法对于彩色图像的隐藏比较实用。

- 量化噪声伪装

通过控制预测量化器的量化等级的选择来嵌入图像数据流，而嵌入其中的特定数据对于公开图像而言近似为一种量化噪声，因而不容易以被发现。

基于音频的信息隐藏

- 音频信息隐藏的核心思想是以音频作为隐藏载体，从中找到一些对人耳听觉相对不敏感的音频参数，然后根据待隐藏信息对这些特性的某些参数进行修改，从而实现待隐藏信息在音频中的嵌入，最后将携密音频传输给接收方，完成整个带隐藏信息的保密传输过程。
- 音频信息隐藏的主要技术指标
  - 透明性
  - 鲁棒性
  - 不可检测性
  - 安全性

基于音频的信息隐藏

根据嵌入隐秘信息所使用的域，音频信息隐藏可以分为：

- 时域音频隐藏

直接对音频信号的幅度或音频文件结构进行处理，包括LSB隐藏，回声隐藏以及音频文件结构隐藏等

- 频域音频隐藏

先对音频进行离散傅里叶变换，然后对音频的频域特征进行处理，以实现信息嵌入。包括频域LSB隐藏，扩频隐藏，相位隐藏和频带分隔隐藏等。

- 离散余弦变换（DCT）域音频隐藏

先对音频载体进行DCT变换，然后对DCT系数进行某些操作，从而完成信息嵌入。该方法对数模、模数转换抵抗能力非常强，有很高的的使用价值。

- 小波域音频隐藏
- 压缩域音频隐藏

基于视频的信息隐藏

根据嵌入隐秘信息的嵌入方式或修改的参数，视频信息隐藏可以分为：

- 基于原始视频的信息隐藏

这种方法基于原始视频嵌入信息，秘密信息直接被嵌入视频的源数据，类似于图像信息隐藏算法，嵌入后再对原始视频进行压缩编码。

- 基于压缩域的信息隐藏

这种方法在压缩的视频中嵌入隐藏信息，嵌入时先解码，在编码过程中进行信息隐藏。包括联合预测误差的视频信息隐藏算法、基于MPEG压缩域的视频流信息隐藏算法、基于帧内量化之久系数的信息隐藏等

- 基于码流域的信息隐藏

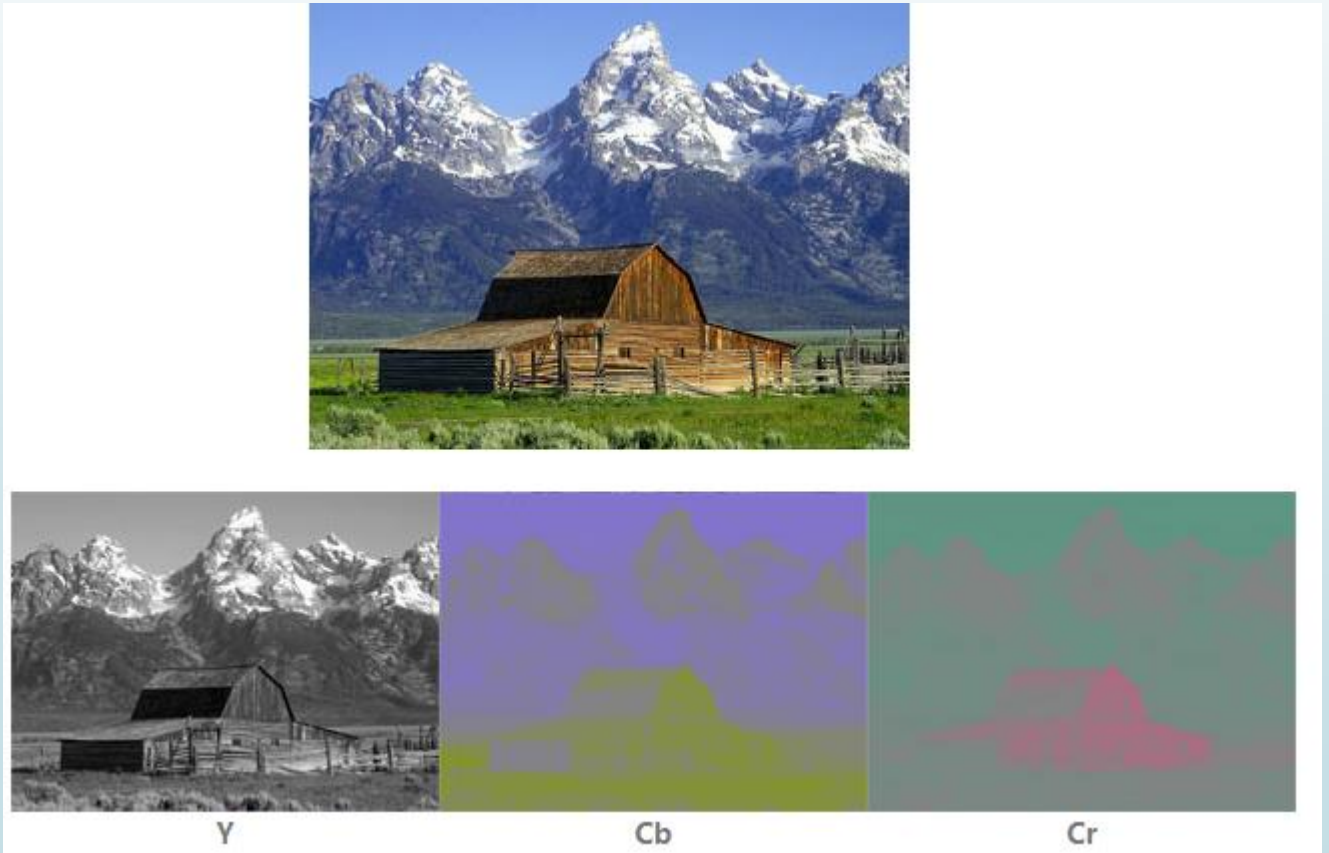
信息直接嵌入视频压缩码流，接收方也直接从码流中提取秘密信息。包括基于MPEG-4纹理编码方案的信息隐藏算法。

基于JPEG压缩域的图像数字水印算法

- 1、把图像分割成大小为8x8不重叠的图像块，这些小块在整个压缩的过程中都是单独被处理。

基于JPEG压缩域的图像数字水印算法

- 2、颜色空间转换，将RGB空间转换为YCbCr空间



基于JPEG压缩域的图像数字水印算法

- 3、对于Y分量进行离散余弦变换。经过DCT变化的图像数据，第一个数据叫做直流系数（DC），之后的数据叫做交流系数（AC）。DC系数表示的是图像中的主要区域，AC系数表示的是图像中的轮廓的细节部分。

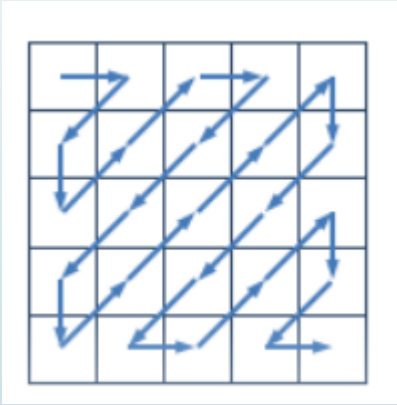
$$\begin{bmatrix} 100 & 100 & 100 & 100 & 100 & 100 & 100 & 100 \\ 100 & 100 & 100 & 100 & 100 & 100 & 100 & 100 \\ 100 & 100 & 100 & 100 & 100 & 100 & 100 & 100 \\ 100 & 100 & 100 & 100 & 100 & 100 & 100 & 100 \\ 100 & 100 & 100 & 100 & 100 & 100 & 100 & 100 \\ 100 & 100 & 100 & 100 & 100 & 100 & 100 & 100 \\ 100 & 100 & 100 & 100 & 100 & 100 & 100 & 100 \\ 100 & 100 & 100 & 100 & 100 & 100 & 100 & 100 \end{bmatrix} \xrightarrow{DCT} \begin{bmatrix} 800 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

基于JPEG压缩域的图像数字水印算法

- 4、数据量化。经过DCT变换之后的数据需要使用标准的量化表进行量化计算。量化的公式为：B = G / Q 。B代表的是量化后的结果。G为输入值。Q为量化系数。由于人眼对亮度分量较为敏感，因此选择亮度矩阵进行量化。

$$\begin{bmatrix} 16 & 11 & 10 & 16 & 24 & 40 & 51 & 61 \\ 12 & 12 & 14 & 19 & 26 & 58 & 60 & 55 \\ 14 & 13 & 16 & 24 & 40 & 57 & 69 & 56 \\ 14 & 17 & 22 & 29 & 51 & 87 & 80 & 62 \\ 18 & 22 & 37 & 56 & 68 & 109 & 103 & 77 \\ 24 & 35 & 55 & 64 & 81 & 104 & 113 & 92 \\ 49 & 64 & 78 & 87 & 103 & 121 & 120 & 101 \\ 72 & 92 & 95 & 98 & 112 & 100 & 103 & 99 \end{bmatrix}$$

标准亮度量化表



基于JPEG压缩域的图像数字水印算法

- 5、 嵌入原理
- （1）图像的低频分量，图像中主要的信息都保存在低频信息中，低频分量决定了图像的灰度等级。
- （2）图像的中频分量，中频信息决定了图像的基本结构，是图像的主要结构。
- （3）图像的高频分量，高频信息是图像的边缘和细节，是对图像中频信息的进一步强化。

$$G = \begin{bmatrix} -415.38 & -30.19 & -61.20 & 27.24 & 56.12 & -20.10 & -2.39 & 0.46 \\ 4.47 & -21.86 & -60.76 & 10.25 & 13.15 & -7.09 & -8.54 & 4.88 \\ -46.83 & 7.37 & 77.13 & -24.56 & -28.91 & 9.93 & 5.42 & -5.65 \\ -48.53 & 12.07 & 34.10 & -14.76 & -10.24 & 6.30 & 1.83 & 1.95 \\ 12.12 & -6.55 & -13.20 & -3.95 & -1.87 & 1.75 & -2.79 & 3.14 \\ -7.73 & 2.91 & 2.38 & -5.94 & -2.38 & 0.94 & 4.30 & 1.85 \\ -1.03 & 0.18 & 0.42 & -2.42 & -0.88 & -3.02 & 4.12 & -0.66 \\ -0.17 & 0.14 & -1.07 & -4.19 & -1.17 & -0.10 & 0.50 & 1.68 \end{bmatrix}$$

基于JPEG压缩域的图像数字水印算法

- 5、 将嵌入信息的Y分量重新放回YCbCr空间再变换回RGB空间。