

# 数字内容安全

曹 刚

[gangcao@cuc.edu.cn](mailto:gangcao@cuc.edu.cn)



# 课程内容

第1章 概述

第2章 消息认证与数字签名

第3章 感知哈希

第4章 信息隐藏

第5章 数字取证

# 第3章 感知哈希

## 3.0 传统哈希的局限

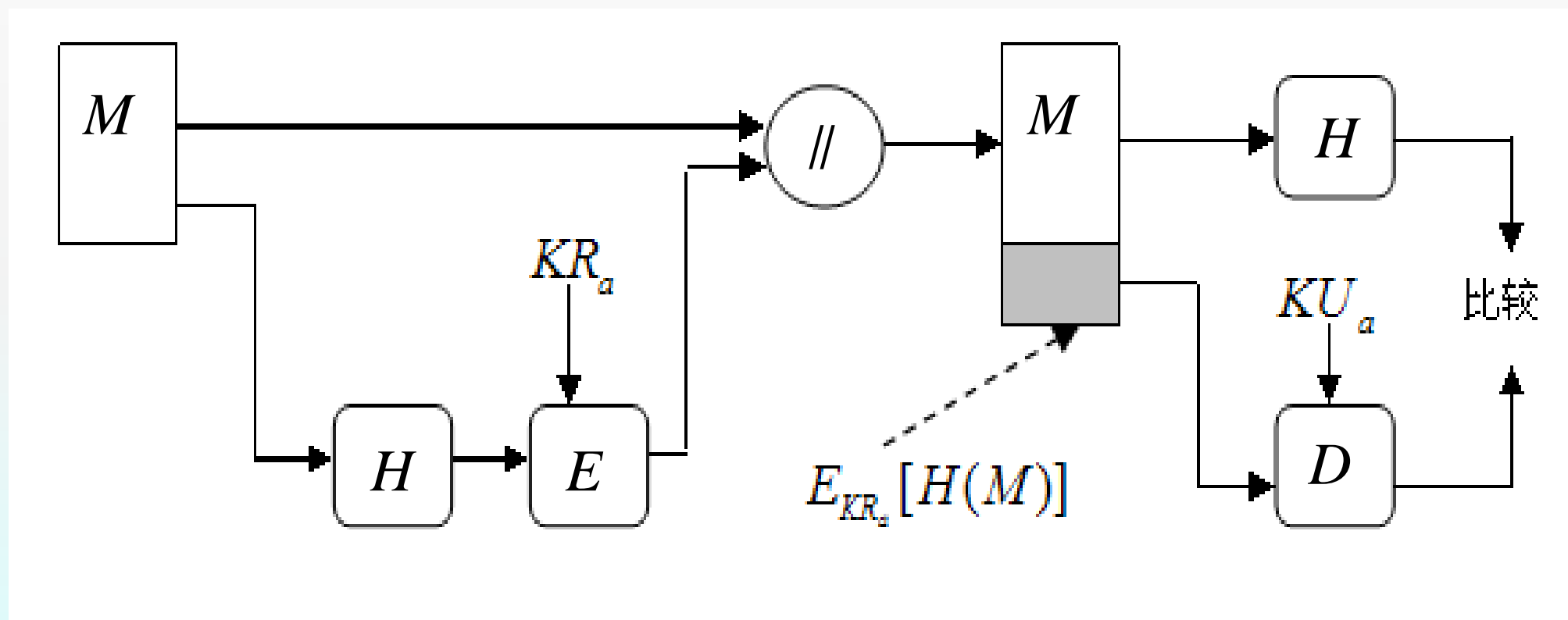
### 3.1 感知哈希概念

### 3.2 感知哈希技术

### 3.3 典型应用

# 传统哈希

## ➤ RSA数字签名算法



◇  $H$ : Hash函数, 输出定长的Hash码

# 传统哈希的局限

## ➤ 定义

- ◆ 哈希函数(Hash Functions)不可逆的提取原始数据的数字摘要(Digest), 具有单向性、脆弱性等特点, 可保证原始数据的唯一性与不可篡改性

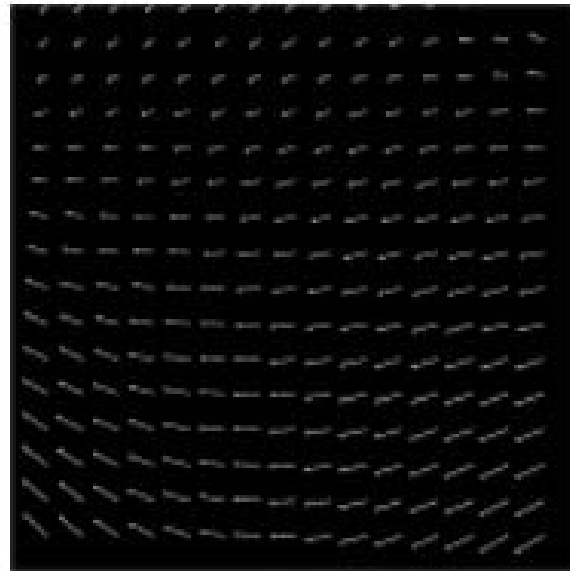
## ➤ 局限

- ◆ 已无法满足多媒体信息管理和保护的需求
- ◆ 多媒体的感知冗余需要有针对性的摘要技术. 传统哈希函数仅具有数据压缩性, 不能消除多媒体感知内容上的冗余
- ◆ 多媒体数字化表示(Digital Presentation)与该媒体内容(Multimedia Content)之间的多对一映射特性, 要求内容摘要具有感知鲁棒性. 而传统哈希函数对任何数字表示改变都是脆弱的

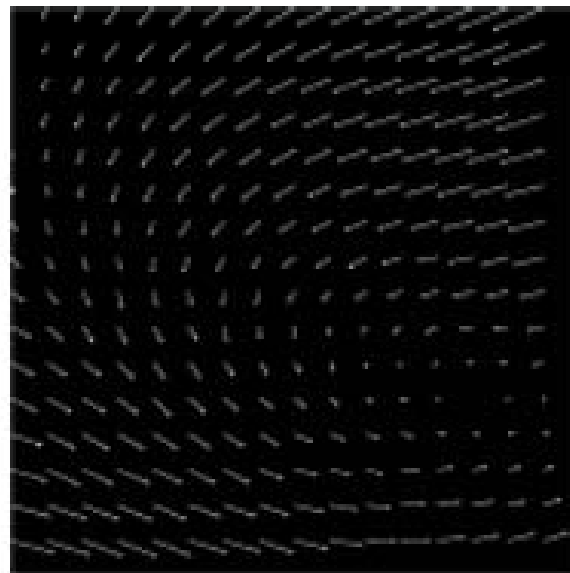
# RBA: an example 多媒体数字化表示 vs 媒体内容



Original



Stirmark 1



Stirmark 2



Example 1



Example 2



# 多媒体数字化表示 vs 媒体内容

## Example: robustness



Addition of white gaussian noise with variance = 2000

# 多媒体数字化表示 vs 媒体内容

## Example: robustness



Print, copying and scanning



# 第3章 感知哈希

3.0 传统哈希的局限

3.1 感知哈希概念

3.2 感知哈希技术

3.3 典型应用



# 感知哈希

## ■ 起始：Ton Kalker 2001 首次提出

- 感知哈希应该是这样一个函数：“它能
  - ◇ 将大数据量的多媒体对象映射为长度较小的比特序列；
  - ◇ 将感知相近的媒体对象映射成数学相近的哈希值。”
- 应用场景之一：**基于内容的媒体访问**（识别-检索-认证）
  - ◇ Ton Kalker 给出了感知哈希的一个令人振奋的应用场景
  - ◇ 你坐在车里收听着电台的音乐。忽然，一首好听的歌深深的吸引了你。它是如此的动听以至于你马上就想知道它的歌名，演唱者，专辑，以及你能够在哪儿能够买到它。然而，你错过了之前关于这首歌的介绍。怎么办？你可以给电台打电话，但是你可能觉得这样太麻烦了。通过感知哈希的支持，你或许只需要在你的手机上简单的按几个钮，等一小会儿，手机就会告诉你这一切，甚或一份详尽的说明已经送到了你的电子信箱里。

# 感知哈希

## ■ 提出与发展

- 必须根据多媒体区别于一般计算机数据的特性, 研究满足多媒体内容压缩性、感知鲁棒性的多媒体单向摘要算法与技术.
- 感知哈希(Perceptual Hashing)已成为多媒体信号处理与多媒体安全及其相关领域的研究热点.

## ■ 理论基础

- 认知心理学: 人认知多媒体的心理过程

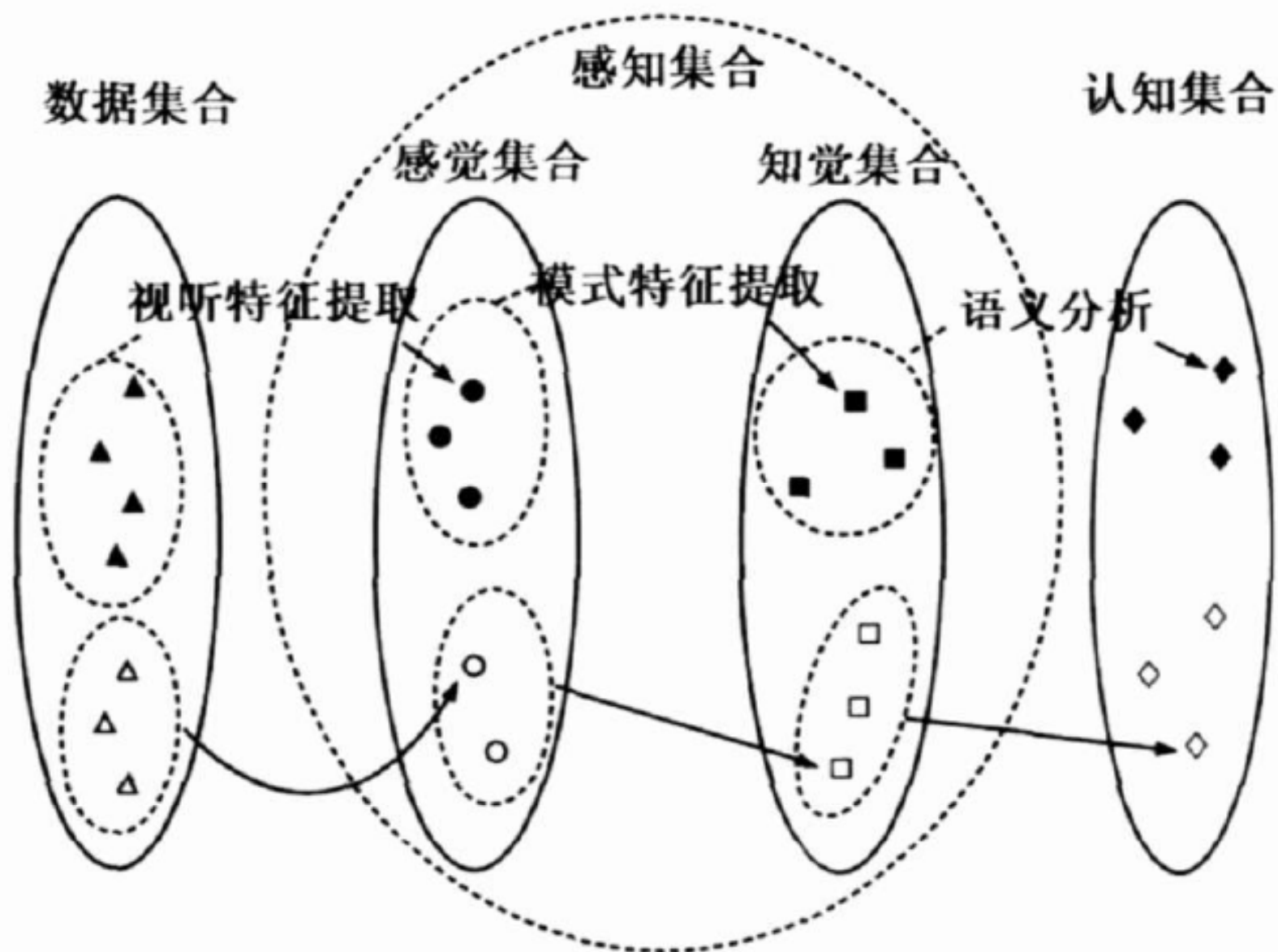
# 感知哈希

## ■ 理论基础

➤ 认知心理学：人认知多媒体的心理过程

表 1 多媒体认知阶段

|            |        |                  |                  |                  |  |
|------------|--------|------------------|------------------|------------------|--|
| 感<br><br>知 | 感<br>觉 | 感<br>知<br>内<br>容 | 感<br>觉<br>内<br>容 | 视<br>听<br>特<br>征 | 人<br>类<br>视<br>觉<br>系<br>统<br><br>心<br>理<br>声<br>学<br>模<br>型 |
|            | 知<br>觉 |                  | 知<br>觉<br>内<br>容 | 模<br>式<br>特<br>征 | 模<br>式<br>识<br>别   |
| 认<br>知     |        | 语<br>义<br>内<br>容 |                  | 语<br>义<br>特<br>征 | 主<br>观<br>分<br>析   |



- ▲ 计算机中存储的多媒体信息的数字表示
- 感觉处理阶段所获得的多媒体信息的视听特征
- 知觉处理阶段所获得的多媒体信息的模式特征
- ◆ 认知处理阶段所获得的多媒体信息的语义特征

图 1 认知各集合及其映射关系



# 感知哈希函数

## ■ 定义

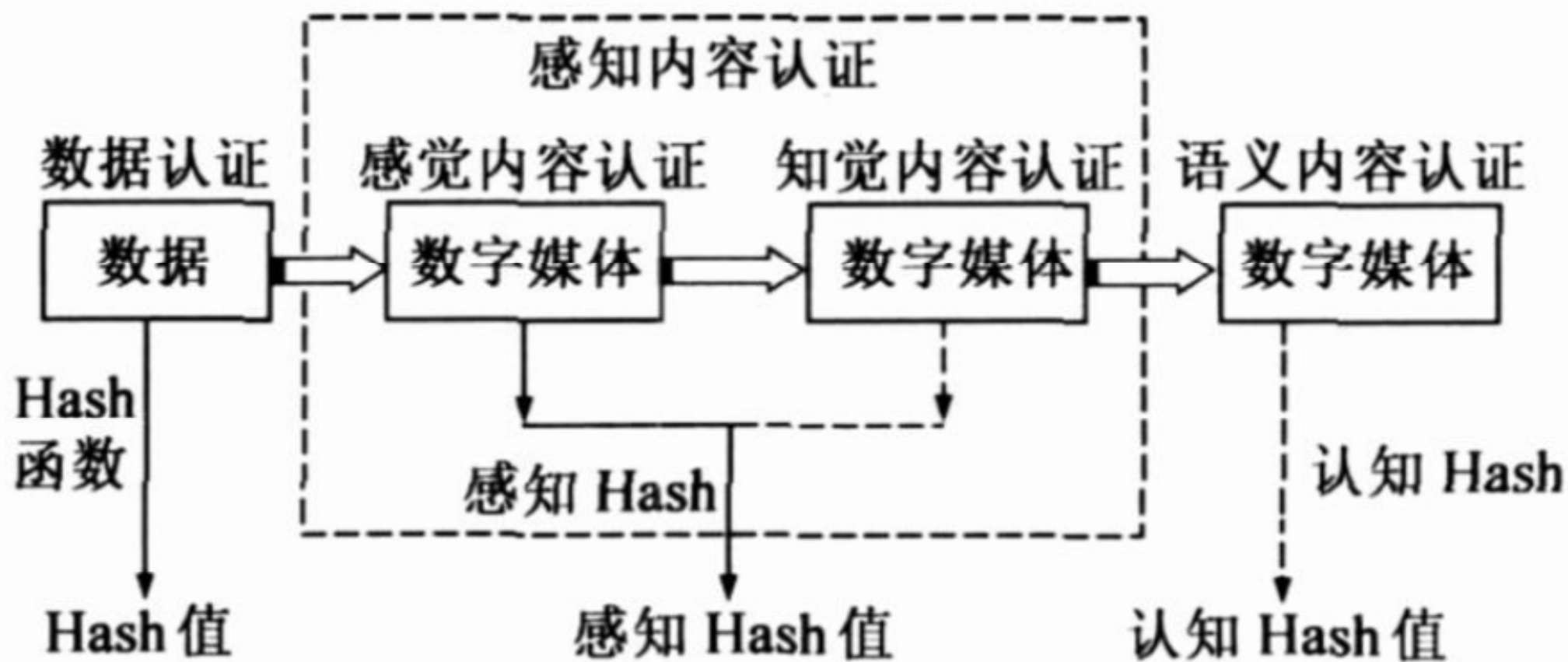
- 感知哈希函数是基于认知心理学的信息加工理论,由多媒体数据集到多媒体感知摘要集的一类单向映射,将具有相同感知内容的多媒体数字表示唯一的映射为一段数字摘要,并满足感知安全性要求.

## ➤ 感知哈希函数

$$PH : M \longrightarrow H_p$$

其中,  $H_p$  为感知数字摘要的集合。

# 传统哈希 vs 感知哈希



# 感知哈希函数的性质

- 抗碰撞性(**Collision Resistance**)/区分性(**Discrimination**)
  - ◈ 内容敏感性
- 感知鲁棒性(**Robustness**)
- 单向性(**One-wayness**)
- 随机性(**Randomicity**)
- 摘要性(**Compactness**)
- 易于实现，计算效率高

# 第3章 感知哈希

3.0 传统哈希的局限

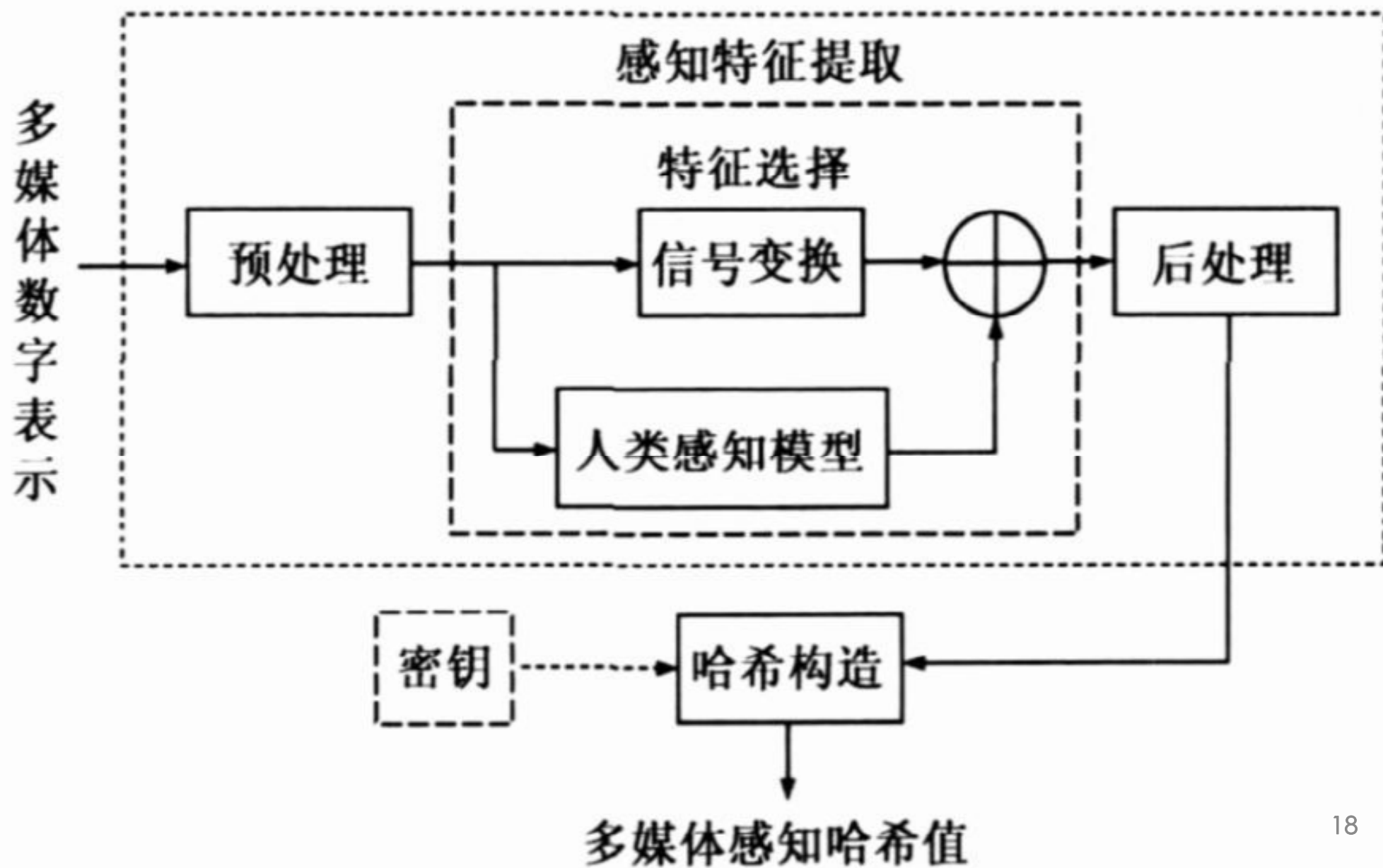
3.1 感知哈希概念

3.2 感知哈希技术

3.3 典型应用



# 感知哈希总体框架





# 感知哈希总体框架

- **预处理：**分帧、滤波等预处理, 可提高特征选择的准确性.
- **感知特征提取：**以人类感知模型为基础, 得到多媒体对内容保持操作的感知不变量.
- **特征选择：**而通过与人类感知模型一致的各种信号处理方法, 可去除感知冗余, 选择最具有感知意义的特征参数.
- **后处理：**为了方便硬件实现, 降低存储要求, 对所选择的特征参数还需进行量化以及编码等后处理.

# 感知哈希总体框架

- **哈希构造：**对感知特征进一步降维,并输出最终结果——感知哈希值.在哈希构造的设计中,必须确保其满足抗碰撞性、单向性、随机性等安全性要求.
- **密钥相依性：**针对应用的不同安全需求,感知哈希可选择不使用密钥以及在不同阶段实现密钥相依性.

# 感知哈希总体框架

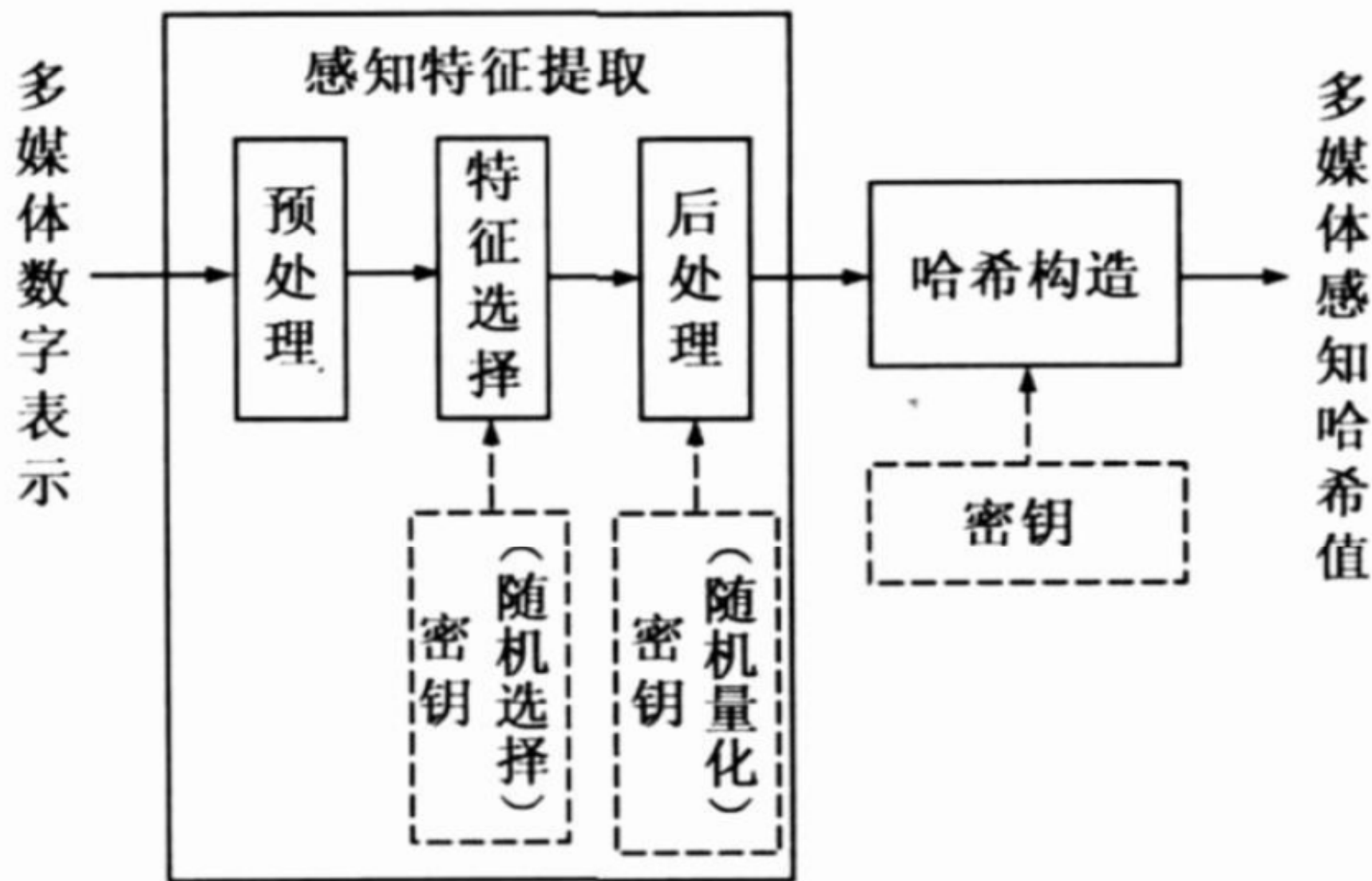
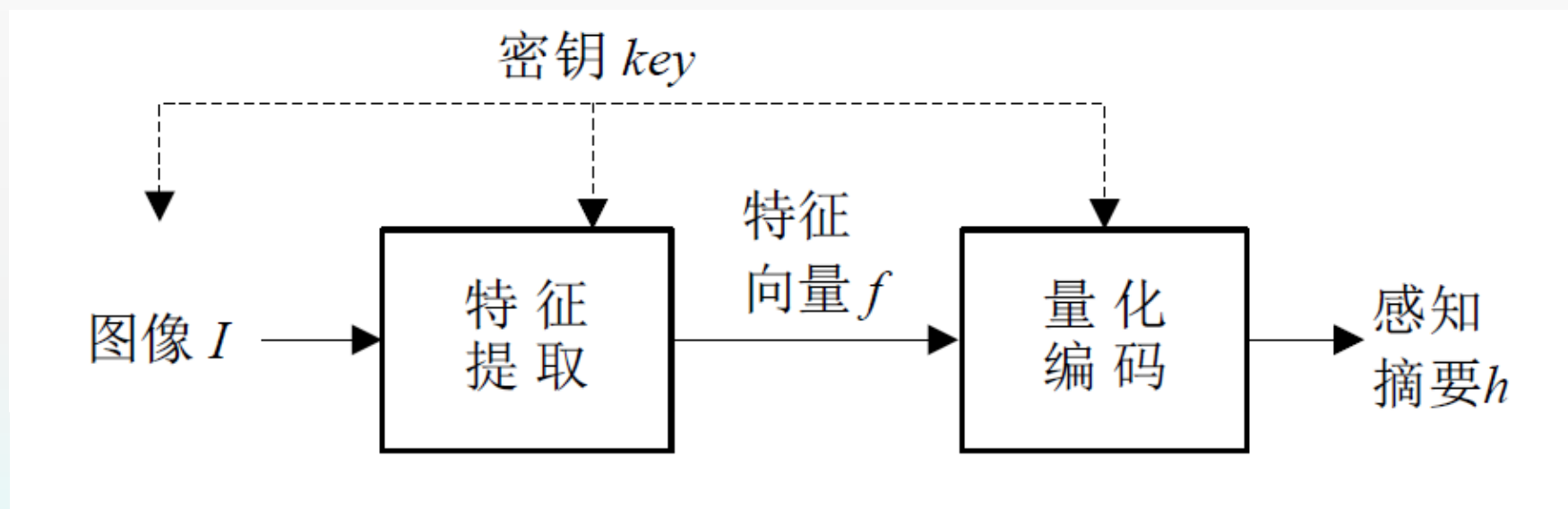


图 4 哈希的密钥相依性构造

# 感知哈希算法

## ➤ 生成算法：



## ➤ 匹配算法：对比两个感知摘要。

# 感知哈希算法

## ➤ 典型方法的分类

- ◆ 基于空域特征：如亮度、图像分块
- ◆ 基于变换域特征：如DFT、DCT、DWT、Fourier-Mellin
- ◆ 矩阵分解：如SVD，NMF
- ◆ 细节特征：如特征点，包括角点、SIFT等

参考文献：

- [1]牛夏牧，焦玉华。感知哈希综述，电子学报，2008
- [2]张慧。图像感知哈希测评基准及算法研究，哈工大博士学位论文，2009
- [3]胡媛媛。基于视觉模型的图像感知哈希算法研究，哈工大博士学位论文，2011
- [4]刘兆庆。图像感知哈希若干关键技术研究，哈工大博士学位论文，2013



# 感知哈希算法

## ➤ 典型方法的另一种分类

### ◆ 基于图像统计特性的特征

- ◆ 利用了图像块直方图的均值、方差和高次惯量等统计不变性属性

### ◆ 基于关系的特征

- ◆ 基于DCT、DWT等变换系数之间的相对大小关系

### ◆ 原始图像粗略特征

- ◆ 利用图像粗略特征对感知的显著性。提取的粗略特征包括：低频DCT系数、低分辨率的小波系数、SVD的最强奇异矢量、Fourier-Mellin变换的旋转不变性

### ◆ 基于边缘或特征点的低层图像特征

# 感知哈希技术

## ➤ 与鲁棒哈希技术的异同

- ◇ 二者最为接近
- ◇ 鲁棒哈希是以任意不变量的选择为建立映射的基础
- ◇ 感知哈希技术以多媒体感知特征为不变量

## ➤ 与数字指纹技术的异同

- ◇ 数字指纹的定义和使用较为混乱
- ◇ 数字指纹主要分为两类：
  - ◆ 应用于版权保护的数字水印技术；
  - ◆ 应用于媒体内容识别的媒体摘要技术。（感知哈希与此类似）

# 第3章 感知哈希

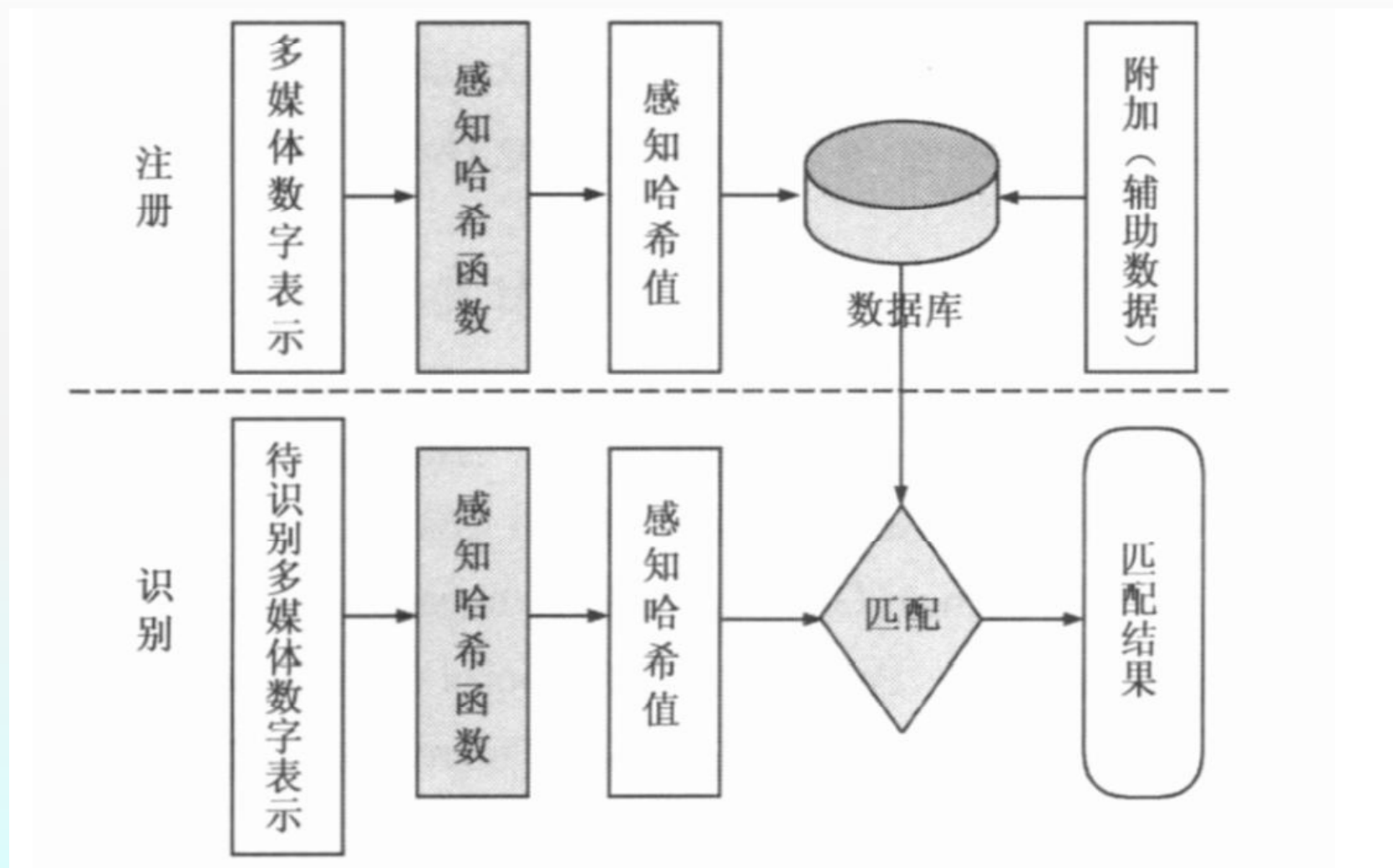
3.0 传统哈希的局限

3.1 感知哈希概念

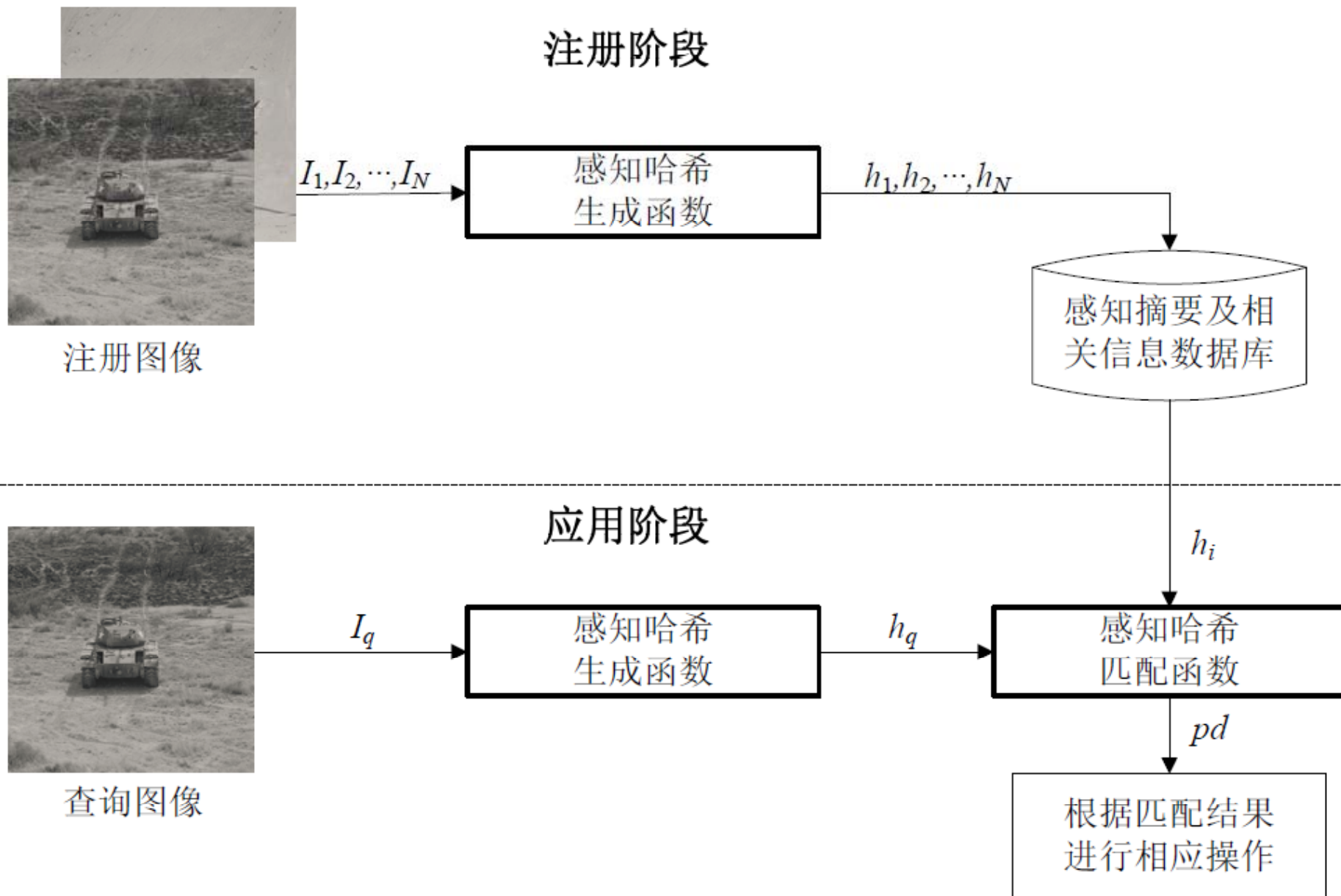
3.2 感知哈希技术

3.3 典型应用

# 1. 识别

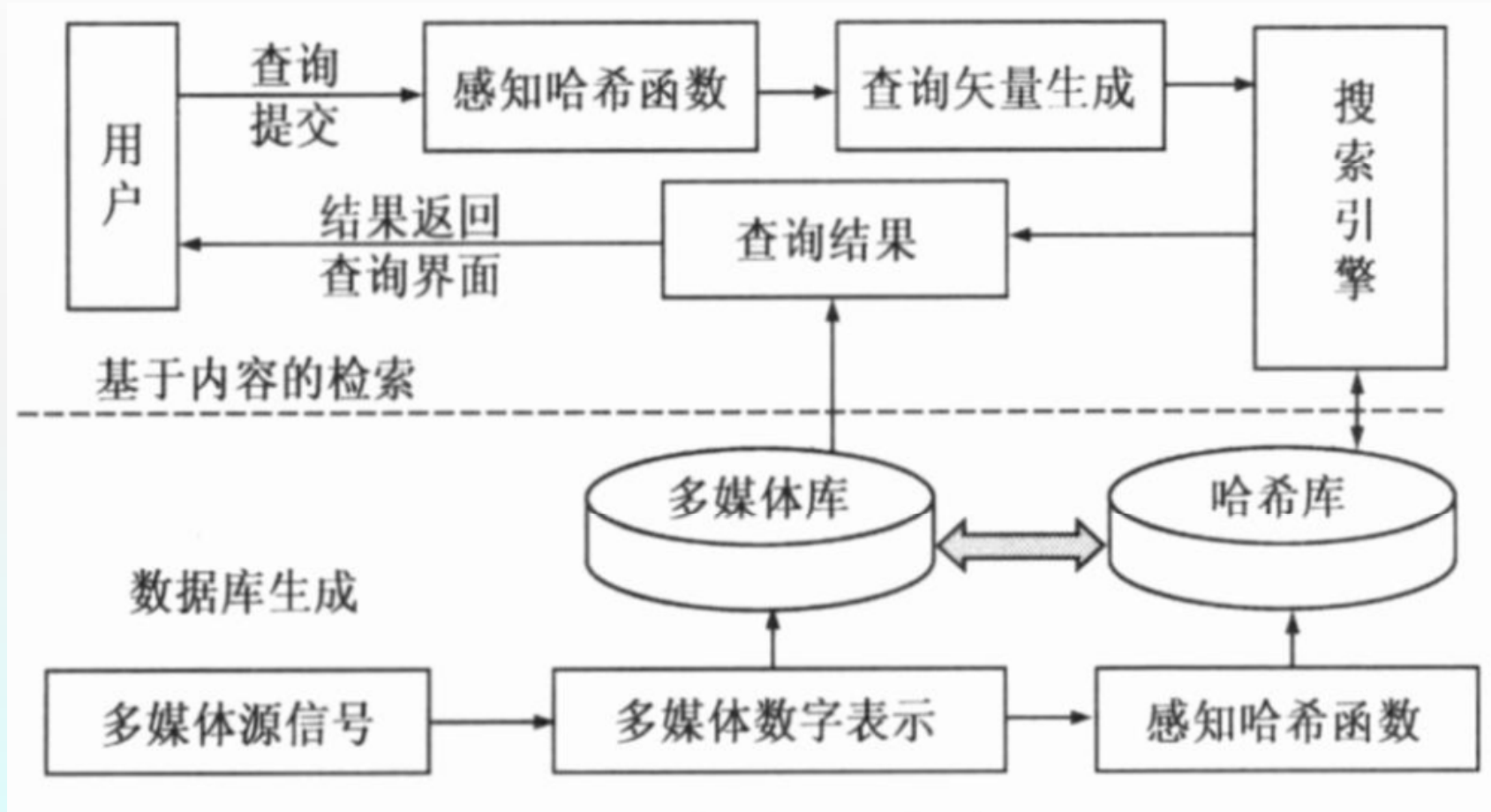


# 1. 识别

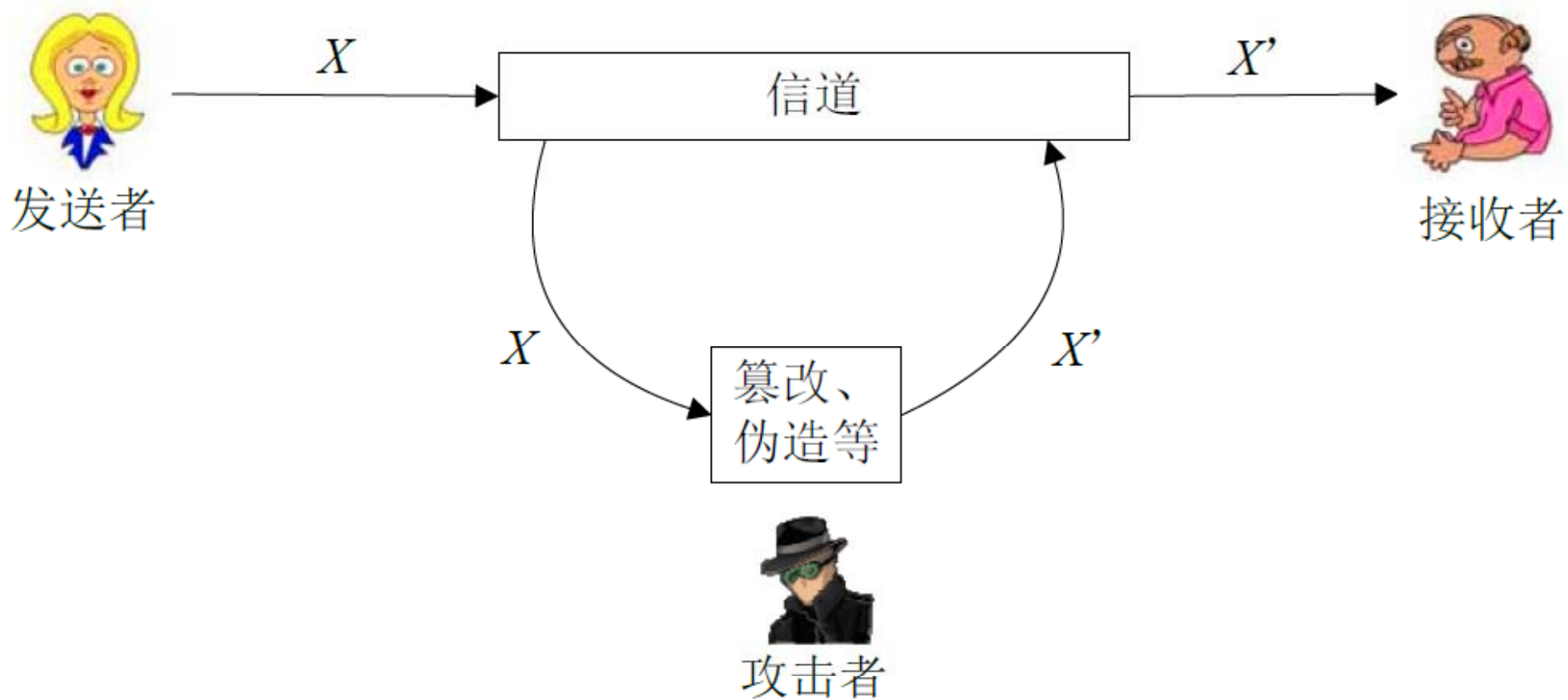




## 2. 检索

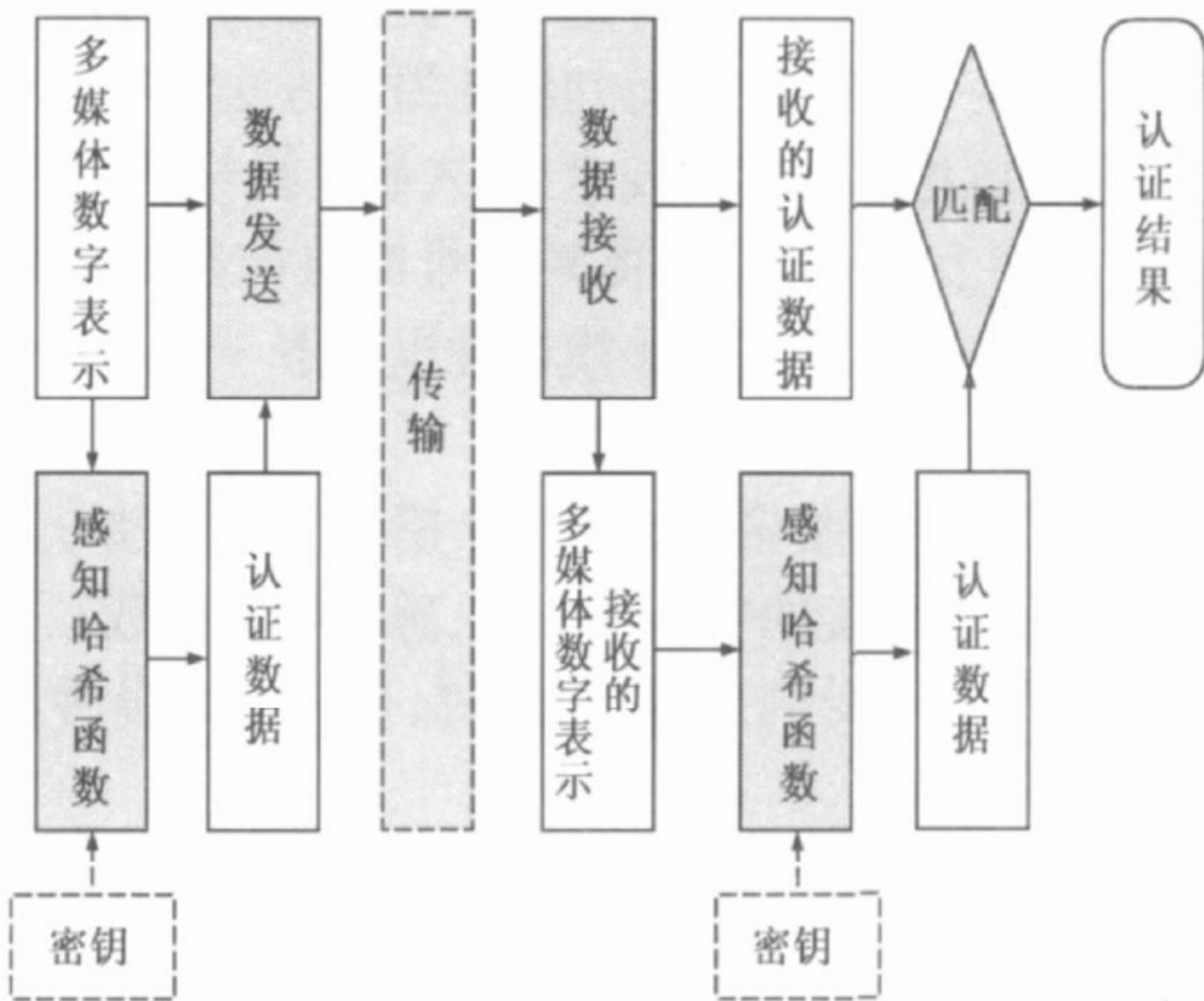


### 3. 认证

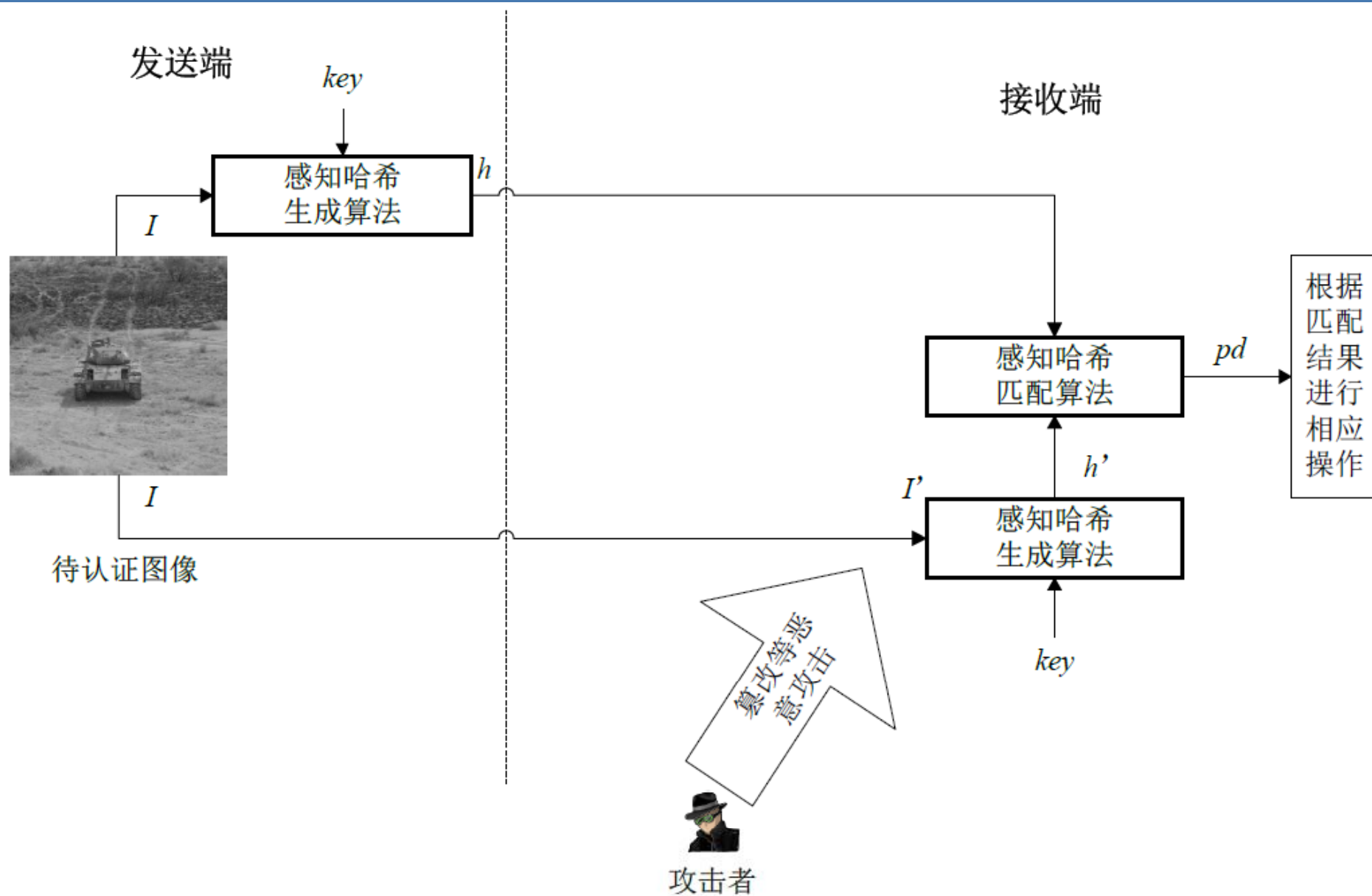


针对认证的多媒体通信系统模型

### 3. 认证

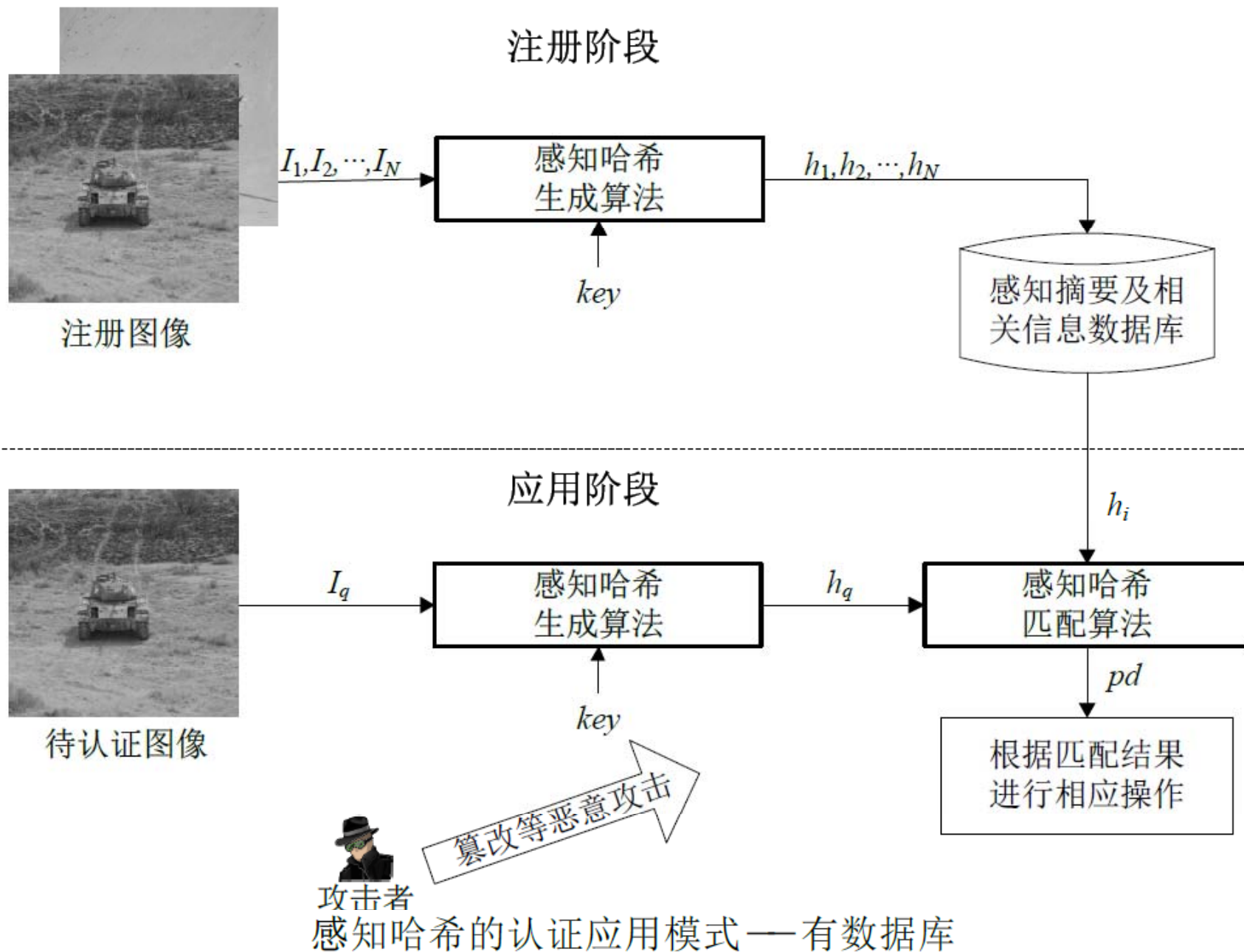


# 3. 认证

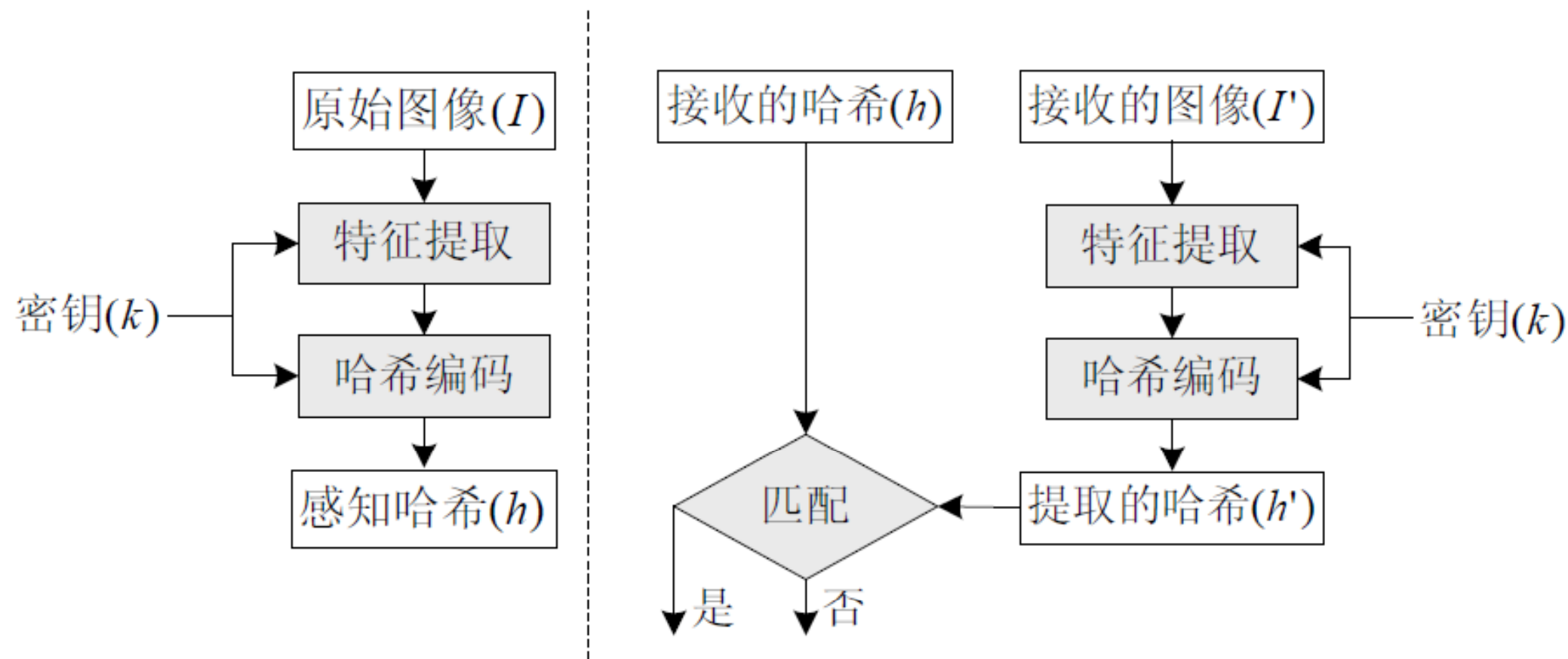


感知哈希的认证应用模式——无数据库

# 认证



### 3. 认证



基于感知哈希的图像认证



# 第3章 感知哈希

## An Example on Image Authentication

IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 17, NO. 12, DECEMBER 2008

2413

### Region-Level Image Authentication Using Bayesian Structural Content Abstraction

Wei Feng and Zhi-Qiang Liu



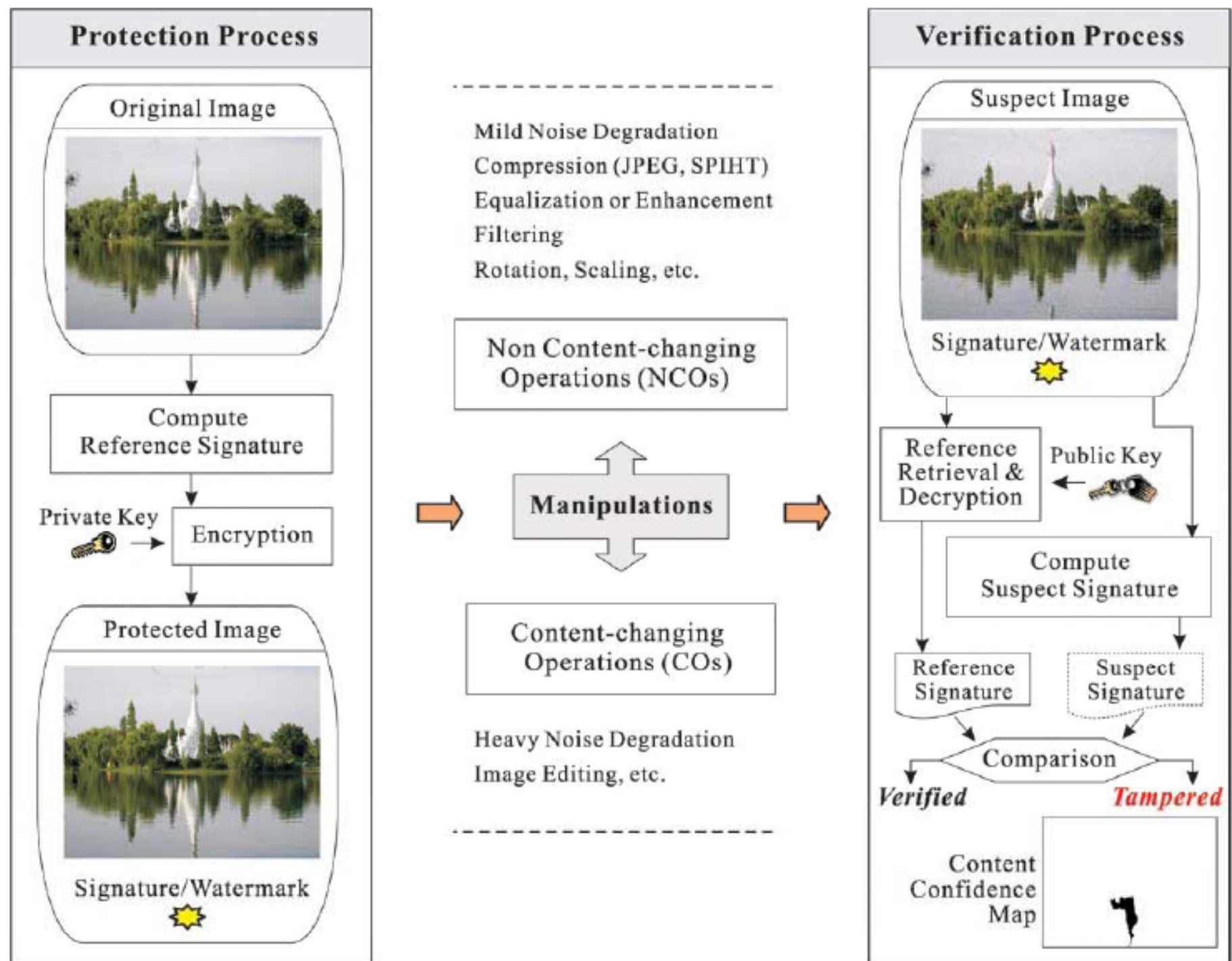


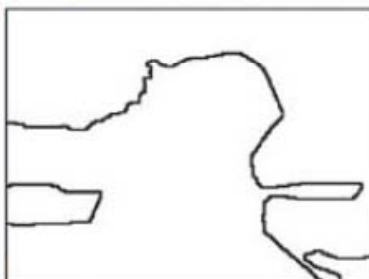
Fig. 1. General diagram of image content authentication.

$X$

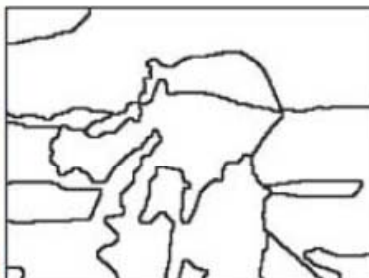


$K$

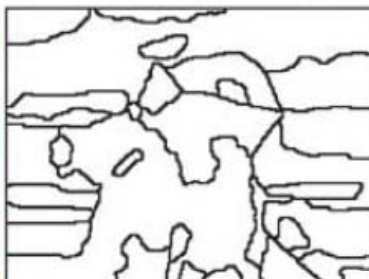
iter#1


























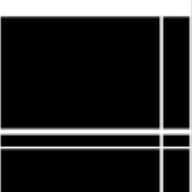
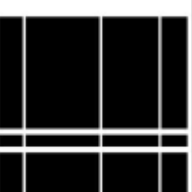


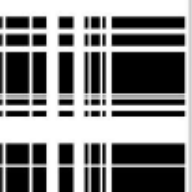

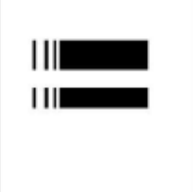








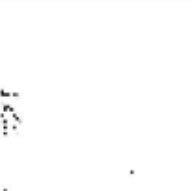










iter#3



iter#7



| Original  | JEPG<br>10%   | JEPG<br>80%   | SPIHT<br>10%   | Media<br>Filtering  | Gaussian<br>Noise 10%   | Scaling<br>25%  | CO #1   | CO #2   |
|---|---|---|--|---|---|---|---|---|
|  |    |    |    |    |    |    |    |    |
| SDS   |    |    |    |    |    |    |    |    |
| JIS   |    |    |    |    |    |    |    |    |
| IMAC  |   |   |   |   |   |   |   |   |
| IH  |  |  |  |  |  |  |  |  |
| BaSCA   |  |  |  |  |  |  |  |  |



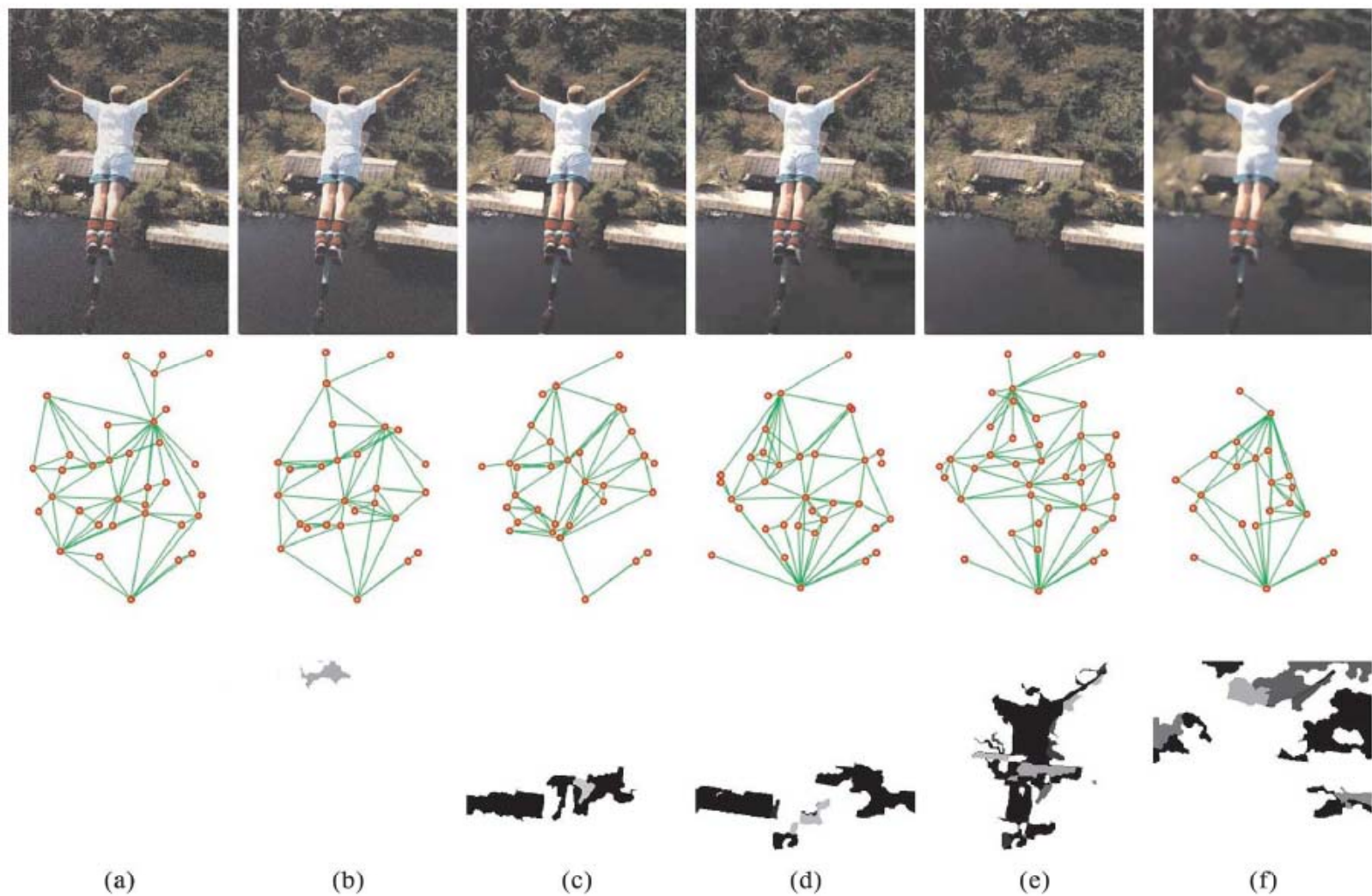


Fig. 10. Verification for unlisted NCOs and composite attacks. The first row is suspect images manipulated by: (a) 20% JPEG + 8% Gaussian noise; (b) 30% random line removal + 7% Gaussian noise; (c) object replacement + 20% SPIHT compression; (d) object replacement + 20% JPEG compression; (e) object deletion + 30% random line removal + 15% JPEG compression; (f) median blurring with  $7 \times 7$  template. The next two rows are corresponding BaSCA signatures and verification results, respectively.

# 第3章 感知哈希

3.0 传统哈希的局限

3.1 感知哈希概念

3.2 感知哈希技术

3.3 典型应用

