

Journal of Image  
and Graphics

# 中国图象图形学报



ISSN1006-8961  
CN11-3758/TB

2012 **6**  
Vol.17 No.

中国科学院遥感应用研究所  
中国图象图形学学会主办  
北京应用物理与计算数学研究所

# 中国图象图形学报

Zhongguo Tuxiang Tuxing Xuebao

2012年6月 第17卷 第6期(总第194期)

## 目次

### 综述

人脸图像的年龄估计技术研究 ..... 王先梅, 梁玲燕, 王志良, 胡四泉(603)

图像统计模型参数估计中的期望最大值算法 ..... 李旭超(619)

### 图像处理和编码

鲁棒的梯度驱动图像修复算法 ..... 叶学义, 王靖, 赵知劲, 陈华华(630)

快速去块效应的线性规划方法 ..... 金剑秋, 刘春晓, 王勋, 章志勇(636)

DWT-SVD 域全盲自嵌入鲁棒量化水印算法 ..... 叶天语(644)

Mean-shift 滤波和直方图增强的图像弱边缘提取 ..... 冀峰, 高新波, 谢松云(651)

### 图像分析和识别

梯度点对约束的结构化车道检测 ..... 王永忠, 王晓云, 文成林(657)

多水平外区抑制的轮廓检测 ..... 闫超, 张建州(664)

基于局部投影与块 LBP 特征的图像检索 ..... 邹彬, 潘志斌, 胡森(671)

### 图像理解和计算机视觉

视觉陌生度驱动的增量自主式视觉学习算法 ..... 瞿心昱, 姚明海, 顾勤龙(678)

霍夫空间中多足球机器人协作目标定位算法 ..... 许家铭, 解仑, 王志良, 倪善超(687)

### 计算机图形学

虚拟 CCD 线阵星载光学传感器内视场拼接 ..... 张过, 刘斌, 江万寿(696)

“第八届数字电视与无线多媒体通信国际论坛”会议专栏

追踪盗版者的抗共谋数字指纹 ..... 李晓强, 张煌, 赵洋洋, 汪晶晶(702)

LBP 与鉴别模式结合的热红外人脸识别 ..... 谢志华, 伍世虔, 方志军(707)

电影中复杂事件的检索与识别 ..... 杜吉祥, 郭一兰, 翟传敏(712)

方向特征和网格特征融合的离线签名鉴别 ..... 杨丹凤, 吕岳(717)

视觉关注度的立体图像质量评价 ..... 张艳, 安平, 张秋闻, 张兆杨(722)

低开销的异构数据交换 ..... 赵凯, 赵正德(726)

灵活的多视点视频编码预测结构 ..... 张艳, 蔡灿辉(730)

跨层反馈在无线视频自适应编码中的应用 ..... 王垚中, 郑世宝, 张重阳, 刘勃(736)

中国图象图形学报

刊名题字: 宋 健

月刊(1996 年创刊)

第 17 卷 第 6 期

2012 年 6 月 16 日出版

<b>主管单位</b> 中国科学院	<b>Superintended by</b> Chinese Academy of Sciences
<b>主 办</b> 中国科学院遥感应用研究所 中国图象图形学学会 北京应用物理与计算数学研究所	<b>Sponsored by</b> Institute of Remote Sensing Application, CAS China Society of Image and Graphics Institute of Applied Physics and Computational Mathematics
<b>主 编</b> 李小文	<b>Chief editor</b> LI Xiaowen
<b>编辑出版</b> 《中国图象图形学报》编辑出版委员会 北京 9718 信箱 邮编 100101 电子信箱:jig@irsa. ac. cn 电话:010-64807995 010-82614429 网 址:www. cjjg. cn	<b>Editor, Publisher</b> Editorial and Publishing Board of Journal of Image and Graphics (P. O. Box 9718, Beijing 100101, China) E-mail:jig@irsa. ac. cn
<b>印刷装订</b> 北京北林印刷厂	<b>Distributed by</b> Beijing Bureau for Distribution of Newspapers and Journals
<b>广告经营许可证</b> 京朝工商广字第 0346 号	<b>Domestic</b> All Local Post Offices in China
<b>总 发 行</b> 北京报刊发行局	<b>Foreign</b> China International Book Trading Corporation (P. O. Box 399, Beijing 100044, China)
<b>订 购</b> 全国各地邮局	<b>Printed by</b> Beijing Beilin Printing House
<b>国外发行</b> 中国国际图书贸易总公司 (中国国际书店) (北京 399 信箱 邮编 100044)	

ISSN 1006-8961 CN11-3758/TB CODE ZTTFXZ 国内邮发代号: 82-831 国外发行代号: M1406 国内定价: 45.00 元

# Journal of Image and Graphics

(Monthly, Started in 1996)

Vol. 17 No. 6 June 2012

## Contents

### Review

- Age estimation by facial image: a survey ..... Wang Xianmei, Liang Lingyan, Wang Zhiliang, Hu Siqian(603)  
Expectation maximization method for parameter estimation of image statistical model ..... Li Xuchao(619)

### Image Processing and Coding

- Robust gradient driving image inpainting method ..... Ye Xueyi, Wang Jing, Zhao Zhijing, Chen Huahua(630)  
Fast image de-blocking by linear programming ..... Jin Jianqiu, Liu Chunxiao, Wang Xun, Zhang Zhiyong(636)  
Perfectly blind self-embedding robust quantization-based watermarking scheme in DWT-SVD domain ..... Ye Tianyu(644)  
Weak edge detection using Mean-shift filtering and histogram enhancement ..... Ji Feng, Gao Xinbo, Xie Songyun(651)

### Image Analysis and Recognition

- Gradient-pair constraint for structure lane detection ..... Wang Yongzhong, Wang Xiaoyun, Wen Chenglin(657)  
Contour detection based on multilevel inhibition ..... Yan Chao, Zhang Jianzhou(664)  
Image retrieval method based on local projection and block LBP feature ..... Zou Bin, Pan Zhibin, Hu Sen(671)

### Image Understanding and Computer Vision

- Visual novelty driven incremental and autonomous visual learning algorithm ..... Qu Xinyu, Yao Minghai, Gu Qinlong(678)  
Target localization algorithm for cooperative multi-soccer robots based on Hough space .....  
..... Xu Jiaming, Xie Lun, Wang Zhiliang, Ni Shanchao(687)

### Computer Graphics

- Inner FOV stitching algorithm of spaceborne optical sensor based on the virtual CCD line .....  
..... Zhang Guo, Liu Bin, Jiang Wangshou(696)

### Special Issue of the IFIC' 2011

- Anti-collusion fingerprinting scheme capable of tracing pirate ..... Li Xiaoqiang, Zhang Huang, Zhao Yangyang, Wang Jingjing(702)  
Infrared face recognition using LBP and discrimination patterns ..... Xie Zhihua, Wu Shiqian, Fang Zhijun(707)  
Recognize and retrieval complex events in real movies ..... Du Jixiang, Guo Yilan, Zhai Chuanmin(712)  
Off-line signature verification based on combination of direction feature and grid feature ..... Yang Danfeng, Lv Yue(717)  
Stereo image quality assessment based on visual attention ..... Zhang Yan, An Ping, Zhang Qiuwen, Zhang Zhaoyang(722)  
Low overhead of heterogeneous data exchange ..... Zhao Kai, Zhao Zhengde(726)  
Flexible prediction structure for multi-view video coding ..... Zhang Yan, Cai Canhui(730)  
Cross-layer feedback based adaptive coding for wireless video transmission .....  
..... Wang Yaozhong, Zheng Shibao, Zhang Chongyang, Liu Bo(736)

中图法分类号: TP309 文献标识码: A 文章编号: 1006-8961(2012)06-0702-05

论文引用格式: 李晓强, 张煌, 赵洋洋, 汪晶晶. 追踪盗版者的抗共谋数字指纹[J]. 中国图象图形学报, 2012, 17(6): 702-706.

## 追踪盗版者的抗共谋数字指纹

李晓强, 张煌, 赵洋洋, 汪晶晶

上海大学计算机工程与科学学院, 上海 200072

**摘要:** 利用数字指纹能够追踪非法使用多媒体内容用户。为此提出一种结合 OFFO(正交向量构造最优聚焦指纹)指纹和 BIBD(均衡不完全区组设计)编码的数字指纹方案。该方案以连续型 OFFO 指纹为基向量原型,并在保持不同指纹码间距离不变的情况下把连续型指纹量化为二值指纹,然后利用 BIBD 编码构造出新的多层编码指纹方案。理论分析和实验结果表明,与同类指纹方案相比,新的指纹方案在用户容量相同的情况下有更好的抗共谋攻击能力。

**关键词:** 数字指纹;OFFO;BIBD;盗版追踪;共谋攻击

### Anti-collusion fingerprinting scheme capable of tracing pirate

Li Xiaoqiang, Zhang Huang, Zhao Yangyang, Wang Jingjing

School of Computer Engineering and Science, Shanghai University, Shanghai 200072, China

**Abstract:** Digital fingerprinting is a technique for identifying users who use multimedia content for unintended purposes. This paper develops a new fingerprinting scheme based on OFFO (Optimal Focused Fingerprints from Orthogonality) and BIBD (Balanced Incomplete Block Design). This scheme considers OFFO as basic signal and transforms the continuous code into antipodal form of binary code, and uses balanced incomplete block designs to construct multilayer fingerprinting. Theoretical analysis and experimental results demonstrate that, compared with the similar fingerprinting scheme, the proposed scheme can more exactly identify at least one of colluders with the same user number.

**Key words:** digital fingerprint; optimal focused fingerprints from orthogonality (OFFO); balanced incomplete block designs (BIBD); tracing pirate; collusion attack

## 0 引言

随着网络技术的发展,网络数据传输的速度越来越快,图片、视频等多媒体数据的传输也变得十分方便。但是另一方面,网络的便捷性也令盗版作品的传播变得十分容易,盗版越来越猖獗。数字指纹技术作为一种新兴的反盗版技术,逐渐成为研究热点并得到广泛应用<sup>[1-3]</sup>。通过在作品出售前嵌入购买者的身份信息(数字指纹),当发现盗版后,通过指纹追溯到购买者,从而查找到盗版的源头。这样

购买者便不敢将购买的作品用于盗版,对盗版者形成威慑,起到阻止盗版的作用。而盗版者则为避免被抓到,必然要去破坏作品中的数字指纹信息。数字指纹主要面临来自多个盗版者的共谋攻击。如何提高抗共谋攻击能力是数字指纹研究的主要内容。

目前的数字指纹方案按照对嵌入假设<sup>[4]</sup>的解释不同可分为两种<sup>[5]</sup>:一种是离散型数字指纹,在编码的过程中包含了离散编码的步骤,该指纹设计方案认为不可见位<sup>[4]</sup>是不可改变的,或者只容忍很少的改变,其代表是 c-secure 码<sup>[4]</sup>;另一种是连续型数字指纹,这种指纹未采用嵌入假设,每一位取值范

收稿日期:2011-09-22;修回日期:2012-01-07

基金项目:上海市自然科学基金项目(10ZR1411700);上海市教委重点学科项目(J50103)

第一作者简介:李晓强(1973—),男,副教授,2004年于复旦大学获得计算机应用技术专业博士学位,主要研究方向为信息隐藏与数字水印,图像处理与模式识别,计算机视觉。E-mail:xqli@shu.edu.cn

围是实数,而不像离散型数字指纹每位只能取有限种状态。

近年来,各种文献中所提出的连续型指纹方案主要分为3类:

1) 正交指纹<sup>[6-7]</sup>,其编码的每一位取值是服从高斯分布的实数,每个用户的指纹是相互正交的。检测算法通过比较非法传播媒体文件中提取出的指纹与每个用户对应的指纹相似程度的相关系数来判断哪些用户参与了共谋。如果一个用户参与了共谋,则该用户对应的指纹与提取出的指纹相关系数较大。

2) 最优聚焦指纹(OFF)<sup>[8-9]</sup>,文献给出一种满足 OFF 要求的  $n$  维单形体( $n$ -simplex)连续型指纹,当参与共谋攻击的人数远远小于宿主信号长度的平方根时, $n$ -simplex 指纹能够抓住至少一个共谋者的概率要大于正交指纹。

3) 使用正交向量构造最优聚焦指纹<sup>[10]</sup>(OFFO 指纹),其构造简单,并且能够在共谋发生时以更大的概率抓住至少一个共谋者,性能优于正交指纹和  $n$ -simplex 指纹。另外,文献[11]提出一种基于频分复用的数字指纹技术,虽然构造简单,但其抗共谋攻击的能力是依赖于较长的码字长度,当用户人数为  $N$  时,需要使用  $4N$  的码字长度。而正交指纹的码字长度与用户人数相等即可。文献[12]指出了正交指纹的缺点,即表示不同用户的信息,需要大量的正交基向量。

为进一步提高数字指纹方案的抗共谋攻击能力,并在给定基向量的情况下容纳更多的用户,提出一种结合 OFFO 指纹和均衡不完全区组设计的数字指纹多层编码方案。该方案以连续型 OFFO 指纹为基向量原型,并在保持不同指纹码间距离不变的情况下把连续型指纹量化为二值指纹,然后利用 BIBD (均衡不完全区组设计) 编码构造出新的多层编码指纹方案。理论分析和实验结果表明,与同类指纹方案相比,在用户容量相同的情况下,本文方案有更好的抗共谋攻击能力。

## 1 数字指纹的构造方案

### 1.1 OFFO 指纹

OFFO<sup>[10]</sup>是在正交向量的基础上构造的一组指纹编码,其具体构造方法如下:

设  $\{Q_i\}$  ( $i = 1, 2, \dots, M$ ) 是一组正交向量,则 OFFO 码中的第  $i$  个指纹编码为

$$P_i = \sqrt{\frac{M}{M-1}} \left( \frac{Q_i}{\|Q_i\|} - \frac{1}{M} \sum_{j=1}^M \frac{Q_j}{\|Q_j\|} \right) \quad (1)$$

由式(1)可计算出 OFFO 码有性质

$$P_i^T P_j = \begin{cases} -\frac{1}{M-1} & i \neq j \\ 1 & i = j \end{cases} \quad (2)$$

从式(2)可以看出,不同用户指纹之间的相关度为  $-1/(M-1)$ ,相关度仅与用户的总数有关而与指纹的长度无关,这样在构造指纹时,就可以根据用户的数量来构造指纹  $M$ 。在检测时,正确判断用户是否参与共谋的难易程度就不像  $n$ -simplex 指纹和正交指纹那样完全受制于指纹编码的长度  $N$ 。并且  $M < N$ ,所以  $-1/(M-1) < -1/N < 0$ ,这也表明不同 OFFO 指纹之间的相关度差异比  $n$ -simplex 指纹和正交指纹的大,因此更容易辨别一个用户是否参与了共谋。

### 1.2 BIBD 编码方案

BIBD 是组合数学中研究的一项内容,定义如下:

**定义 1** 集合  $\mathcal{X}$  有  $v \geq 2$  个元素, $\mathcal{X}$  有  $b > 0$  个子集,每个子集称为一个区组(Block),如果某种设计满足:

- 1) 每个区组中包含  $k$  个元素;
- 2) 每个元素包含在  $r$  个区组中;
- 3) 每对元素同时出现在  $\lambda$  个区组中。

则称满足以上条件的设计为  $(v, b, r, k, \lambda)$ -BIBD。对于  $(v, b, r, k, \lambda)$ -BIBD 有如下性质:

- 1)  $bk = vr$ ;
- 2)  $r(k-1) = \lambda(v-1)$ 。

根据以上性质可以很容易看出, $b$  和  $r$  完全可以由  $v, k, \lambda$  来表示。所以  $(v, b, r, k, \lambda)$ -BIBD 可以简写为  $(v, k, \lambda)$ -BIBD。

某个元素在某一个子集出现用 1 表示,未出现用 0 表示,则一个  $(v, k, \lambda)$ -BIBD 可以和一个矩阵  $R = \{r_{ij}\}$  相对应,其中

$$r_{ij} = \begin{cases} 1 & \text{第 } i \text{ 个元素属于第 } j \text{ 个子集} \\ 0 & \text{其他} \end{cases}$$

$R$  的每行对应  $\mathcal{X}$  中的一个元素,每列对应一个子集。

### 1.3 结合 OFFO 和 BIBD 的多层指纹编码方案

首先选择  $v$  个 OFFO 基  $u_1, \dots, u_v$ ,再将矩阵  $R$  中的 0 映射成 1,1 映射为  $-1$ 。然后将向量  $\{u_1, \dots, u_v\}$  和经过映射变换后的  $R$  其每一列求内积作为分配给用户的指纹信息。对于  $(7, 3, 1)$ -BIBD 相关矩阵  $R_1$

$$R_1 = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}$$

若分配给用户  $i$  的指纹为  $P_i$ , 则

$$P_1 = -u_1 - u_2 + u_3 - u_4 + u_5 + u_6 + u_7$$

$$P_2 = -u_1 + u_2 - u_3 + u_4 + u_5 - u_6 + u_7$$

⋮

$$P_7 = u_1 + u_2 + u_3 - u_4 - u_5 - u_6 + u_7$$

若令  $U = \{u_1, \dots, u_v\}$ ,  $R'$  表示  $R$  映射后的矩阵,  $P = \{P_1, P_2, \dots, P_M\}$ , 则  $P = UR'$ 。

在介绍检测算法前先给出一个抗“与”共谋码 (AND-ACC)<sup>[12]</sup> 定义。

**定义 2** 令  $G = \{0, 1\}$ , 一个码向量集  $C = \{c_1, c_2, \dots, c_M\} \in G^N$ , 若满足小于等于  $k$  个元素

的子集进行逻辑与运算得到的结果不同于其他任何小于等于  $k$  个元素子集的逻辑与的结果, 则  $C$  是抗“与”共谋的。

Trappe 等人<sup>[12]</sup> 证明对于一个 BIBD 来说, 其相关矩阵  $R$  列向量构成的码字的集合是抗“与”共谋的。对于  $(v, k, \lambda)$  - BIBD 能够抗  $(k - 1)$  个用户的“与”共谋。

表 1 是一个  $(16, 4, 1)$  - BIBD 抗“与”共谋码的例子, 其中  $(16, 4, 1)$  - BIBD 的相关矩阵为  $R_2$  用户 1, 4, 8 的码分别是相关矩阵  $R_2$  的第 1, 4, 8 列经过映射后的结果。由于  $(16, 4, 1)$  - BIBD 是抗 3 个用户“与”共谋的, 所有任何其他两个用户的码的平均都不同于用户 1, 4 码的平均值。对 3 个用户的情况也一样。

提取出盗版作品中的指纹后, 盗版者检测的过程分两步: 1) 确定一个向量  $\Gamma = \{\Gamma_i\}$ , 其中  $\Gamma_i \in \{0, 1\}$ , 具体的确定方法是将每一个基  $u_i$  代入到式(3)中的检测器

$$R_2 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

表 1 两个或者 3 个抗“与”共谋码参与平均攻击

Table 1 Average collusion attack with two or three users

用户 1	-1	-1	-1	-1	1	1	1	1	1	1	1	1	1	1	1	1	1
用户 4	-1	1	1	1	1	1	1	1	1	1	-1	-1	-1	1	1	1	1
用户 8	1	-1	1	1	1	1	-1	1	-1	1	1	1	1	1	-1	1	1
用户 1,4 平均	-1	0	0	0	1	1	1	1	1	1	0	0	0	1	1	1	1
3 个用户平均	-1/3	-1/3	1/3	1/3	1	1	1/3	1	1/3	1	1/3	1/3	1/3	1	1/3	1	1
3 个用户平均后, 经阈值划分	0	0	0	0	1	1	0	1	0	1	0	0	0	1	0	1	1

$$T_N(\mathbf{u}_i) = \frac{\mathbf{Y}^T \mathbf{u}_i}{\sqrt{\|\mathbf{u}_i\|^2}} \quad (3)$$

$\mathbf{Y}$ 表示盗版中的指纹信息。若 $T_N(\mathbf{u}_i) > \tau$ ,  $\Gamma_i = 1$ , 否则 $\Gamma_i = 0$ ; 2) 将 $\Gamma$ 代入硬检测算法中, 该算法伪码如下:

HardDectAlg( $\Gamma$ )

$\Phi = \mathbf{1}$ ;

令 $J$ 为 $\Gamma$ 中 $\Gamma_i = 1$ 的索引的集合

for  $t = 1$  to  $|J|$

$j = J(t)$ ;

令 $\mathbf{e}_j$ 为矩阵 $\mathbf{R}$ 的第 $j$ 列

$\Phi = \Phi \cdot \mathbf{e}_j$

end

return  $\Phi$

$\Phi$ 是一个 $M$ 维向量, 对应于 $M$ 个用户, 每个元素为0或1, 最后得到的 $\Phi$ 中值为1的元素所对应的用户参与了共谋攻击。

## 2 实验结果与讨论

仿真实验主要对文献[12]指纹方案和本文指纹方案的性能进行比较。实验采用(16, 4, 1)-BIBD

码, 在该方案中需要16个基向量, 可以产生满足20个用户的指纹编码。实验步骤如下:

1) 生成指纹 首先分别选取16个正交基和OFFO基。在得到基向量 $\mathbf{U} = \{\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_{16}\}$ 后, 按照 $\mathbf{P} = \mathbf{U} \cdot \mathbf{R}'$ 构造指纹,  $\mathbf{R}'$ 为 $\mathbf{R}$ 映射后的矩阵。指纹的长度 $N = 10\ 000$ 。

2) 共谋攻击 共谋攻击同样是在平均共谋攻击后附加上高斯白噪声。

3) 检测盗版用户 若用1表示用户参与共谋, 0表示未参与共谋, 则检测最终输出结果包括以下4项: (1) 正确识别盗版者的概率 $P(1|1)$ ; (2) 将盗版者判为无辜者的概率 $P(0|1)$ ; (3) 将无辜者判为盗版者的概率 $P(1|0)$ ; (4) 正确识别的无辜者的概率 $P(0|0)$ 。

为减少随机性对实验结果带来的干扰, 把实验重复1000次, 得到的实验结果如图1所示。可以看出随WNR(水印噪声比,  $WNR = 10 \lg \|\mathbf{P}_i\|^2 / \|\mathbf{d}\|^2$ ,  $\|\mathbf{P}_i\|^2$ 和 $\|\mathbf{d}\|^2$ 分别表示指纹、噪声的能量)的增大, 噪声的作用逐渐减弱, 两种指纹方案中判断错误的概率 $P(1|0)$ 和 $P(0|1)$ 随之下降, 判断正确的概率 $P(1|1)$ 和 $P(0|0)$ 随之上升。另外, 从图1中可以看出, 当WNR值大于-25时, 在相同的

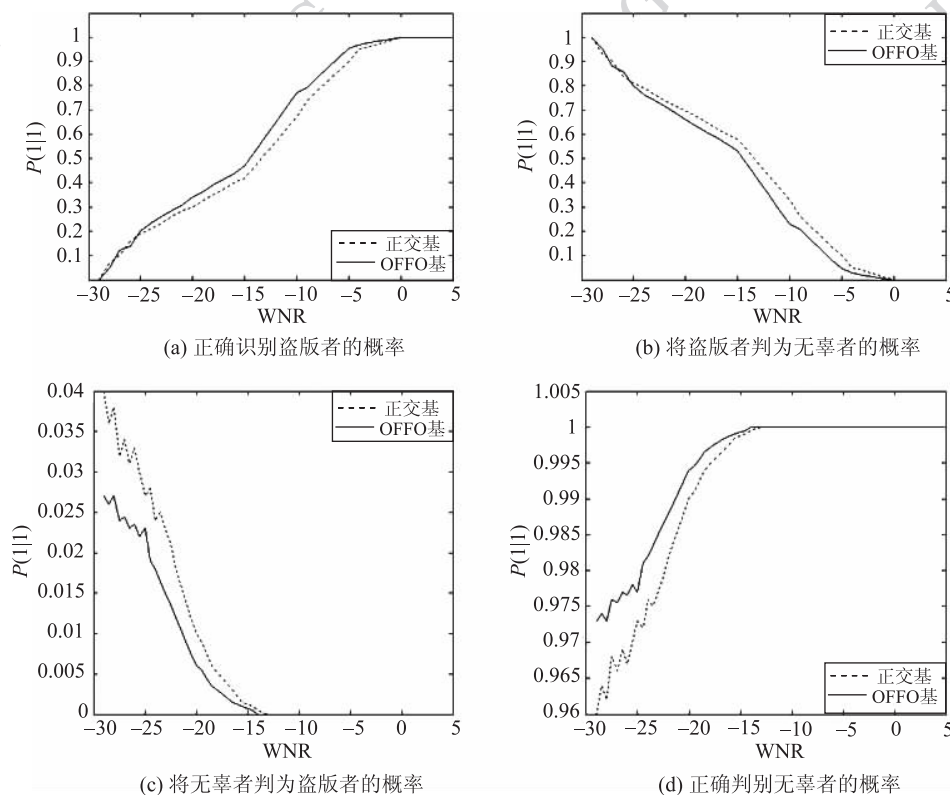


图1 指纹方案性能测试

Fig. 1 Performance test of the fingerprint scheme

WNR 下,相对于采用正交基的 BIBD 指纹方案,以 OFFO 为基的多层指纹编码方案能够显著提高正确识别盗版者和无辜者的概率,同时降低混淆无辜者和盗版者的概率。这说明在用户数量、噪声相同的情况下,本文构造的算法具有更好的抗共谋攻击性能。

### 3 结 论

OFFO 指纹与正交指纹相比,相同指纹的相关度和不同指纹之间的相关度之差比正交指纹的要大,因此比正交指纹更容易辨别一个用户是否参与了共谋。在此基础上,结合 OFFO 指纹和 BIBD 编码的多层数字指纹编码方案。理论分析和实验结果表明,该方案能够综合 OFFO 指纹和 BIBD 编码的优点,在相同用户数量和噪声的情况下,以 OFFO 为基的多层指纹方案表现出比正交编码为基的方案更好的抗共谋攻击性能。

数字指纹本质上是数字水印的一种特殊形式,其在实际使用中必须与鲁棒性水印算法结合,利用水印嵌入策略把指纹嵌入到被保护的数据中,从而为音频、图像、视频等多媒体数据的分发系统提供安全保障。

### 参考文献 (References)

- [ 1 ] Lian S, Liu Z. Secure media content distribution based on the improved set-top box in IPTV [ J ]. IEEE Transactions on Consumer Electronics, 2008, 54(2): 560-566.
- [ 2 ] Chen Y, Lin W S, Liu K J R, et al. Risk-distortion analysis for video collusion attacks: A Mouse-and-Cat Game [ J ]. IEEE Transactions on Image Processing, 2010, 19(7): 1798-1807.
- [ 3 ] Varna A L, He S, Swaminathan A, et al. Fingerprinting compressed multimedia signals [ J ]. IEEE Transactions on Information Forensics and Security, 2009, 4(3): 330-345.
- [ 4 ] Boneh D, Shaw J. Collusion-secure fingerprinting for digital data [ J ]. IEEE Transactions on Information Theory, 1998, 44(5): 1897-1905.
- [ 5 ] Li D, Lu Z X, Lu H M. Digital fingerprinting system and marking assumption [ J ]. Computer Science, 2007, 34(11): 68-72. [ 李栋, 卢增祥, 路海明. 数字指纹编码与嵌入假设 [ J ]. 计算机科学, 2007, 34(11): 68-72. ]
- [ 6 ] Cox I J, Killian J, Leighton T. Secure spread spectrum watermarking for multimedia [ J ]. IEEE Transactions on Image Processing, 1997, 6(12): 1673-1687.
- [ 7 ] Wang Z J, Wu M, Zhao H, et al. Anti-collusion forensics of multimedia fingerprinting using orthogonal modulation [ J ]. IEEE Transactions on Image Processing, 2005, 14(6): 804-821.
- [ 8 ] Kiyavash N, Moulin P. Regular simplex fingerprints and their optimality properties [ C ] // Proceedings of International Workshop on Digital Watermarking . Berlin, German: Springer, 2005: 97-109.
- [ 9 ] Kiyavash N, Moulin P, Kalker T. Regular simplex fingerprints and their optimality properties [ J ]. IEEE Transactions on Information Forensics and Security, 2009, 4(3): 318-329.
- [ 10 ] Pan G Y, Li X Q, Li W. Optimal focused fingerprints from orthogonality [ C ] // Proceedings of International Conference on Audio, Language and Image. New York, America: IEEE, 2008, 2: 1640-1644.
- [ 11 ] Yan Z T, Zhang H L. Digital fingerprint scheme based on the FDM-technique [ J ]. Journal of Image and Graphics, 2010, 15(9): 1326-1330 [ 晏钊韬, 张汗灵. 一种基于频分复用的数字指纹技术 [ J ]. 中国图象图形学报, 2010, 15(9): 1326-1330. ]
- [ 12 ] Trappe W, Wu M, Wang J Z, et al. Anti-collusion fingerprinting for multimedia [ J ]. IEEE Transactions on Signal Processing, 2003, 51(4): 1069-1087.