软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2011,22(8):1884−1896 [doi: 10.3724/SP.J.1001.2011.03822]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

基于残留特征跟踪的抗合谋数字指纹*

王祖喜, 王文宗+, 葛 强, 胡汉平

(华中科技大学 图像识别与人工智能研究所,湖北 武汉 430074)

Collusion-Resistant Digital Fingerprinting Based on Residual Characters Tracking

WANG Zu-Xi, WANG Wen-Zong+, GE Qiang, HU Han-Ping

(Institute for Pattern Recognition and Artificial Intelligence, Huazhong University of Science and Technology, Wuhan 430074, China)

+ Corresponding author: E-mail: asooone@yahoo.com.cn, http://www.hust.edu.cn

Wang ZX, Wang WZ, Ge Q, Hu HP. Collusion-Resistant digital fingerprinting based on residual characters tracking. *Journal of Software*, 2011,22(8):1884−1896. http://www.jos.org.cn/1000-9825/3822.htm

Abstract: This paper creates a kind of linear independent character code, presents a new theory based on Synergetic, which applies Synergetic to digital fingerprinting, and then proposes a scheme of collusion-resistant digital fingerprinting based on residual characters tracking. The efficiency and the performance are proved and analyzed by theories and examples. The experimental results indicate that the proposed method can greatly improve the efficiencies of encoding and tracing in the digital fingerprinting. The performance in robustness and collusion-resistant is able to meet the requirements of the applications of digital fingerprinting.

Key words: copyright protection; digital fingerprinting; conspiracy attack; Synergetic; linearly independent character code

摘 要: 通过设计一种数字指纹的线性无关特征码,提出基于协同学的残留特征跟踪的抗合谋数字指纹,将协同学应用于数字指纹的合谋跟踪,建立了一套基于残留特征跟踪的抗合谋数字指纹方案.实验结果及分析表明,该方案能够在大幅度提高数字指纹的编码效率和跟踪效率的同时,基本上保证数字指纹的鲁棒性和抗合谋性.

关键词: 版权保护;数字指纹;合谋攻击;协同学;线性无关特征码

中图法分类号: TP309 **文献标识码**: A

随着多媒体技术和网络技术的迅速发展,各类数字产品的应用越来越广泛.数字产品的易拷贝和易传播等特点,使得数字产品版权保护问题日益突出,并已成为数字世界的一个非常重要和紧迫的问题.数字指纹技术是近几年发展起来的新型数字版权保护技术,主要用来跟踪数字产品非法拷贝和传播的源头,帮助对非法用户进行指控,达到版权保护和威慑非法行为的作用.

目前,针对数字指纹的攻击主要有两种方式:单用户攻击和合谋攻击[1].单用户攻击主要攻击数字指纹的鲁棒性,目的是在不破坏数据对象可用性的前提下破坏或去除数字指纹,攻击手段主要有噪声攻击、剪切、滤波、JPEG 压缩等.合谋攻击是对数字指纹特有的一种攻击方式.抵抗合谋攻击能力是评估一个数字指纹系统的主要

* 基金项目: 国家自然科学基金(60773192); 国家教育部博士点基金(20050487046); 湖北省自然科学基金(2007ABA015); 北京市"现代信息科学与网络技术"重点实验室暨铁道部"铁路信息科学与工程"开放实验室资助项目(XDXX1008)

收稿时间: 2009-02-12; 定稿时间: 2009-12-29; jos 在线出版时间: 2010-09-20

指标.合谋攻击的主要攻击手段有合谋篡改攻击和平均攻击[1].合谋篡改攻击通过比较两份合法作品,找到水印嵌入的位置,然后进行篡改,使自己的非法发布行为无法被跟踪.由于水印嵌入前置乱的方法得到普遍应用,攻击者不能有针对地对指纹进行有意义的篡改,这种攻击手段得到一定程度的抑制.平均攻击是用两份或多份作品线性相加求平均的方法,将数字指纹从作品中抹去,这已经成为最常见的数字指纹攻击手段.

数字指纹研究的热点之一集中于数字指纹的编码,通过抗合谋编码来抵抗合谋攻击.目前数字指纹编码和跟踪大多基于组合论的方法.Fernandez 和 Sorano 提出了一种基于有限几何的指纹编码方案[2],Trappe 等人提出的基于平衡非完全区组设计(balance incomplete block design,简称 BIBD)构造的指纹编码方案也采用了特殊的组合结构[3].Staddon 等人对可确认父元码(identifiable parent property,简称 IPP)、防陷害码(frame proof,简称 FP)、安全防陷害码(secure FP,简称 SFP)、可跟踪码(tracibility,简称 TA)的组合特性及它们的相互联系进行了研究[3];同时,运用组合论和编码理论中的若干方法,讨论了有关码字结构中参数界的问题,并给出了几种关于 IPP 码、TA 码等编码的构造方法[4].

基于组合论的编码保证不同用户组合的合谋可行集均不同,这样,通过比较不同用户合谋后的可行集就可以追踪出合谋的用户.当数字指纹被正确提取出来以后,将其与用户指纹集合比较,如果发现其与某一指纹相同,则可认为找到了非法再分发的用户.如果在指纹集合中没有发现与提取出的指纹相匹配的指纹,则检查其是否在某一合谋可行集中.如果发现这一指纹属于某一合谋可行集,则可通过该合谋可行集跟踪出合谋用户[3,5−7].

基于组合论的数字指纹有一些优点,比如,可以精确地确定多个合谋者;但是也存在一些问题,比如,当提取的指纹有损坏时,可能误将无罪用户检测为合谋者.这主要是因为在提高数字指纹编码码距的同时,很难同时提高合谋可行集间的码距.在提取的指纹有损坏的情况下,有时很难判断提取的指纹属于哪个合谋可行集,错误的判断导致冤枉无辜用户.基于组合论的数字指纹的思想还导致跟踪模式库比用户数庞大得多(用户数为 n、最多容忍 N 个用户合谋的模式库大小至少为 $C_n^1+C_n^2+C_n^3+...+C_n^N$),跟踪算法效率较低[7].

针对基于组合论数字指纹所表现出来的这些不足,本文提出了一种新的数字指纹抗合谋思想——基于残留特征跟踪的数字指纹思想,通过跟踪合谋残留的指纹特征来跟踪合谋者.

1 基于残留特征跟踪的数字指纹抗合谋思想

协同学理论[8]是 20 世纪 70 年代初由德国物理学家 Haken 提出并创立的一门新型学科.在协同模式识别领域,协同神经网络模型已被用于解决 2D 工业零件辨识、手写字符识别、人脸识别、车牌识别等问题[8].

在协同系统中,初始状态的设置表现为部分有序化的子系统,属于这个子系统的序参量在竞争中取胜,最后支配整个系统并使其进入这个特定的有序状态.换言之,一旦给出具有某个模式特征的集合,其中具有最强初始支撑的序参量就获得胜利,并驱使系统呈现模式中原来缺少的特征[8].

如果将多用户合谋产生的合谋模式作为协同系统的输入模式,而数字指纹库组成了协同系统的模式集合,则模式集合中具有最强初始支撑的序参量将获得胜利,该模式就将被选择出来作为匹配的结果.也就是说,合谋指纹中具有特征多的对应用户将被认定为合谋者.

更简单地说就是,多个用户合谋时,谁残留的指纹特征更多,谁就将在协同学的神经网络的竞争中获胜,将被成功地跟踪.这就是基于残留特征跟踪的数字指纹抗合谋思想.

为了达到被合谋攻击时数字指纹的特征不被完全抹去,需要设计相应有效的特征编码.为方便表述,称参与合谋的指纹模式为合谋模式,合谋产生的模式为新模式,指纹库中模式本来就具有的特征称为原始特征,合谋产生的特征称为新特征.该编码必须满足两个条件:

(1) 合谋不能抹去合谋模式的所有原始特征,原始特征仍被尽可能多地保留下来;

(2) 非合谋模式不能与新模式更匹配,即新模式尽可能少地具有指纹库中非合谋模式的特征.

实际上,大多数合谋是不会抹去原始特征的,只不过多个特征叠加起来形成了新特征.如果模式库中没有非合谋模式与新模式更匹配,协同系统会将新特征作为多个合谋模式的原始特征来对待.也可以从序参量的含义上来考虑这个问题:若把输入模式看成原型模式的线性组合,序参量就代表了输入模式对原型模式分解的系数,

输入模式越接近原型模式,这个系数就越大,相应的序参量就越大,在竞争中获胜的可能性也就越大.也就是说,如果不存在非合谋模式与新模式更匹配,在协同系统中合谋产生的新模式就会主要分解在合谋模式上,即新特征就会分解为多个合谋模式的原始特征.以上分析表明,如果条件(2)得到满足,条件(1)也就基本上得到了满足.

为满足上述编码要求,提出线性无关特征码的概念:

对于 N 个向量 $\boldsymbol{R}_i(i=1,2,\ldots,N)$,这里,$\boldsymbol{R}$ 为二进制域向量,如果

$$k_1\boldsymbol{R}_1+k_2\boldsymbol{R}_2+k_3\boldsymbol{R}_3+\ldots+k_N\boldsymbol{R}_N=0 \tag{1}$$

仅当 $k_1=k_2=k_3=\ldots=k_N=0$ 时才成立,那么称这 N 个向量 $\boldsymbol{R}_i(i=1,2,\ldots,N)$线性无关.

如果线性无关的 N 个向量 $\boldsymbol{R}_i(i=1,2,\ldots,N)$满足:

$$\max P(\boldsymbol{R}_i,\boldsymbol{R}_j)\leqslant\alpha,\ i\neq j,\ i,j=1,2,\ldots,N \tag{2}$$

其中,$P(\cdot)$为某种相关性度量函数,α为阈值,那么,称这 N 个向量为特征为α的线性无关特征向量.

在此给出另一种特殊的线性无关特征向量:如果线性无关的 N 个向量 $\boldsymbol{R}_i(i=1,2,\ldots,N)$之间的最小汉明距离满足:

$$\min d(\boldsymbol{R}_i,\boldsymbol{R}_j)\geqslant\beta\cdot L,\ i\neq j,\ i,j=1,2,\ldots,N \tag{3}$$

其中,β为阈值,L 为向量 $\boldsymbol{R}_i$ 的长度,那么,称这 N 个向量为特征差为β的线性无关特征向量.

如果把线性无关特征向量作为数字指纹,则把这种数字指纹编码称为线性无关特征码.

线性无关特征码保证了任意两个码向量之间都存在有效的区分度,在一定程度上避免了数字指纹匹配时误匹配的情况发生.

线性无关特征码保证了任意多个码向量的线性组合都与其他码向量保持一定程度的差异,这样就可以避免非法用户合谋陷害其他用户的可能性.同时,线性无关特征码保证了参与合谋用户的数字指纹的一些特征不被完全抹去,残留的特征多的数字指纹将在协同学的神经网络的竞争中获胜,从而被成功地跟踪.

正交码是一种特殊的线性无关特征码.正交码不仅要求各个码向量之间是线性无关的,而且要求各个码向量之间的内积为 0,即

$$(\boldsymbol{R}_i,\boldsymbol{R}_j)=\begin{cases}1, & i=j\\ 0, & i\neq j\end{cases},\ i,j=1,2,3,\ldots,N \tag{4}$$

正交码对指纹的提取要求较高,它是靠提取的指纹全部特征来精确确定合谋用户的,这必然导致数字指纹的鲁棒性不高.当有误码或者噪声干扰时,有很大可能将无辜合法用户错误地判断为合谋者.

2 基于残留特征跟踪的数字指纹方案

数字指纹方案主要分几个部分来考虑:数字指纹的生成方案、数字指纹的嵌入和提取方案、数字指纹的跟踪方案.

图 1 为基于残留特征跟踪的数字指纹方案图,虚线框中表示了系统中各个部分所采用的方法.

(1) 数字指纹的生成

将用户信息编码为有意义的二值图像,将该二值图像作为指纹.本文将用户序列号编码为该序列号的二值图像.

指纹编码算法流程如下:

① 将用户的身份信息映射为一个数字序列号.

② 确定指纹生成密钥,该密钥决定指纹生成的一些参数,包括二值指纹图像的大小、阿拉伯数字的字体和大小、阿拉伯数字图像在整个二值指纹图像中的位置、各个数字图像之间的距离等.

③ 根据密钥生成数字指纹二值图像.

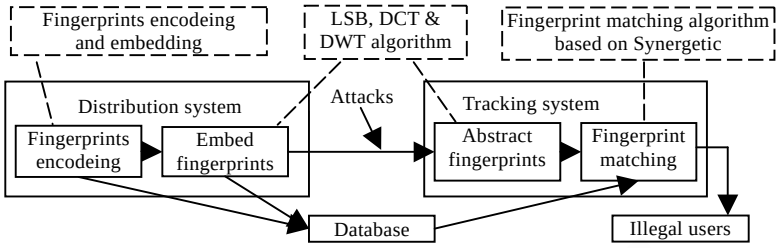


Fig.1 Digital fingerprinting schematic drawing

图 1 数字指纹方案图

图 2 为按上述算法生成的一个数字指纹二值图像.该图像大小为 64×15,阿拉伯数字为宋体小四号.

Fig.2 Digital fingerprint binary image

图 2 数字指纹二值图像

宋体阿拉伯数字 0~9 的图像矩阵如图 3 所示.将每个矩阵的列分别合并为 1 列,得到 10 个向量.容易证明,这 10 个向量是线性无关的.因此,将这 10 个向量分别扩展,它们仍然是线性无关的.所以,按照上述算法生成的数字指纹库是线性无关的.通过计算得出,本文实验中,构造的指纹库的特征差β=6/(15×64)=0.00625,即本文实验中的指纹库是由特征差为 0.006 25 的线性无关特征码构成的.

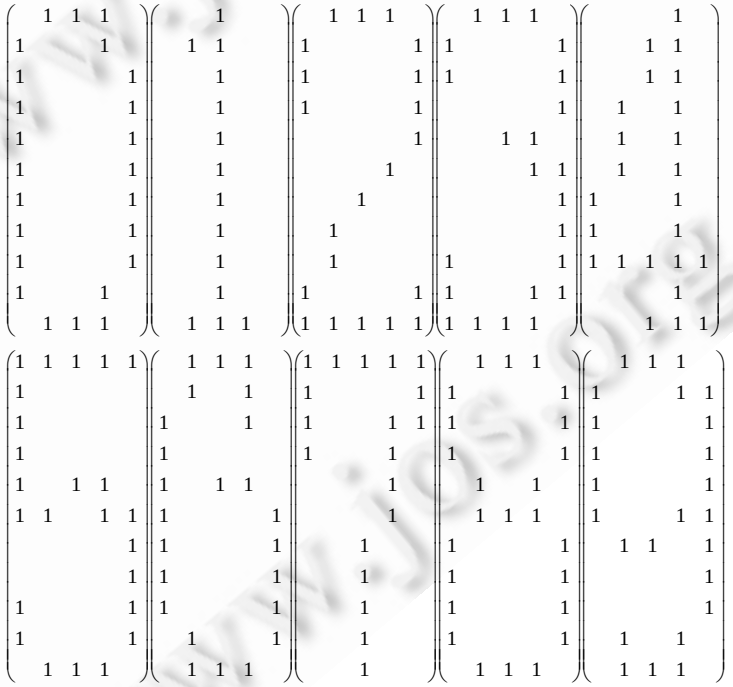


Fig.3 Imaging matrices of 0~9

图 3 0~9 的图像矩阵

这种编码扩展用户很方便,只需扩展数字的位数,每扩展一次可以容纳的用户数都增加为扩展之前的 10

倍,而码长仅增加 1 个阿拉伯数字图像向量的长度.一个阿拉伯数字图像向量的大小取决于阿拉伯数字的字体和大小.本文所作阿拉伯数字字体均为小四号宋体,每个阿拉伯数字编码后数据长度为 11×5=55 位.

(2) 数字指纹的嵌入和提取

本方案中,根据实际应用需求不同可分别在空域和频域中嵌入指纹,如采用 LSB,DCT 和 DWT 算法[9−11]将数字指纹嵌入到图像的中.提取是嵌入的逆过程.

(3) 数字指纹的跟踪

数字指纹跟踪过程就是在跟踪模式库中找到与所提取的指纹相匹配的模式,并确定该指纹模式对应的用户信息的过程.本方案中采用基于协同学的数字指纹匹配算法[12],跟踪模式库就是用户指纹库.

数字指纹模式匹配的步骤如下(如图 4 所示):

① 根据数字指纹嵌入策略提取载体里的数字指纹.

② 对该数字指纹进行模式提取,可以得到模式向量.

③ 对该模式向量进行归一化和零均值处理,得到处理后的新模式向量.

④ 对数字水印库分别进行归一化和零均值处理,得到原型模式向量集和伴随向量.同时求出初始序参量集,并将参数代入协同演化模型进行序参量演化,可以得到新的序参量集.

⑤ 如果序参量中有一个为 1,则待匹配的数字指纹为指纹库中该序参量所对应的那个指纹,结束匹配;否则,转入第 5 步,继续匹配.

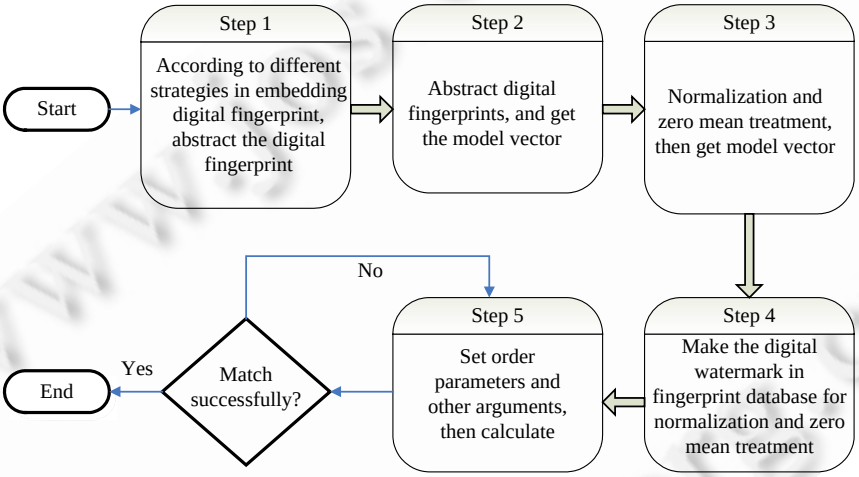


Fig.4 Flow chat of digital fingerprint pattern matching

图 4 数字指纹模式匹配流程

3 仿真实验及分析

本文实验中,用户 *A* 向媒体提供商 SP 购买了数字媒体 Lena 图像.SP 将 *A* 的身份信息映射为一个简单的数字序列 012345,并将该映射信息记录入数据库中.将数字序列 012345 编码为二值图像作为数字指纹,字体采用小四号宋体.为便于实验观测,指纹图像大小为 64×15,图 5 为原图的放大显示.

Fig.5 Digital fingerprint binary image of buyer *A*

图 5 用户 *A* 的数字指纹二值图像

数据库中记录了 Lena 图像的其他购买者,相应数字序列为 012348,812345,012848,072319 等 20 个用户,对应的二值指纹图像如图 6 所示.

Fig.6 Digital fingerprint binary images in Fingerprint Database

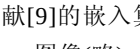
图 6 数字指纹库中的一些二值图像指纹

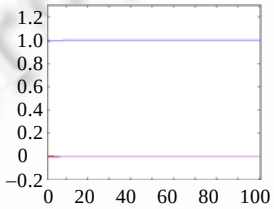
3.1 鲁棒性实验

鲁棒性实验验证在不同嵌入方法下,各种退化操作对指纹残留特征的影响情况,能够发映出何种指纹嵌入及提取方法,能够更多地保留嵌入指纹的残留特征信息,可以更好地达到成功匹配的目的.

(1) LSB 域

实验中,LSB 指纹嵌入借鉴文献[9]的嵌入算法.采用原始 Lena 图像作为载体图像,在其中嵌入数字指纹  ,得到含有数字指纹的 Lena 图像(略).

对含有数字指纹的 Lena 图像不作任何处理,提取指纹得到数字指纹及其序参量演化图,如图 7 所示,其中,图 7(b)中上方的曲线代表了数字指纹  对应的序参量演化曲线.



(a) Digital fingerprint extracted
(a) 提取的数字指纹

(b) Order parameter evolution curves
(b) 序参量演化图

Fig.7 Digital fingerprint and order parameter evolution curves in LSB domain

图 7 LSB 域的数字指纹及对应的序参量演化图

从图 7 中可以看出,未遭受任何攻击的数字指纹与指纹库中指纹的匹配过程很快就完成了,即序参量的演化在极短时间内达到了稳定状态:一个序参量值趋于 1,其他序参量值趋于 0.因为待识别模式与指纹库中某个模式是相同的,所以在演化过程中相应的序参量迅速趋于 1,其他序参量并未出现波动情况而是迅速趋于 0.这也说明基于线性无关特征码的模式库与待识别模式有很好的区分度,能够最大程度地避免误匹配的发生.

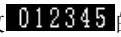
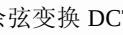
对嵌入数字指纹的 Lena 图像作退化处理,包括高斯噪声、椒盐噪声、剪切、中值滤波等操作.从退化处理后的 Lena 图像中提取数字指纹,对提取的数字指纹进行模式匹配,可得到序参量演化图和匹配结果,见表 1.序参量演化图为提取数字指纹模式的序参量演化曲线,当一条曲线趋向 1 而其他曲线趋于 0 时,表示匹配成功,即趋向 1 的那条曲线所对应的数字指纹与待匹配的数字指纹相匹配;否则,表示匹配失败,即并未找到与待匹配指纹相匹配的指纹.在表 1 第 4 列的序参量演化图中,最后一幅图中上方第 2 根曲线以及其他图中最上方的曲线表示数字指纹  的匹配过程,Lena 图像为原图的缩小显示,数字指纹为原图的放大显示,下同.

表 1 中结果显示,经过椒盐噪声、剪切 1(Cut 1)和中值滤波这些退化操作之后仍然匹配成功,而高斯噪声和剪切 2(Cut 2)操作导致匹配失败.从图 7 中可以看出:前者在规定的演化步数内没有达到稳定状态,判定为匹配失败;而后者对指纹信息破坏较严重,所有的序参量都已经趋于 0,匹配失败.

(2) DCT 域

实验中使用离散余弦变换 DCT 算法,采用原始 Lena 图像作为载体图像嵌入数字指纹  .

对含有数字指纹的 Lena 图像不作任何处理,提取指纹得到数字指纹及其序参量演化图,如图 8 所示.

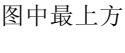
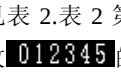
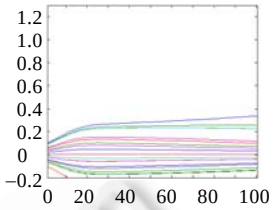
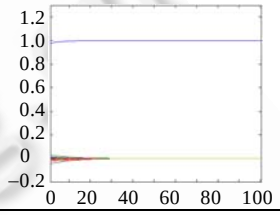
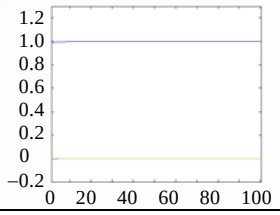
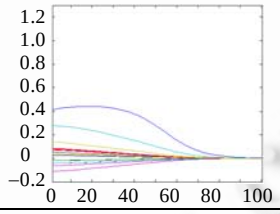
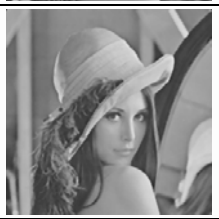
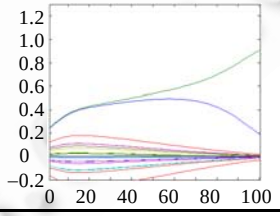
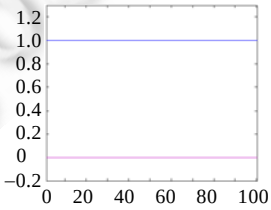
对嵌入数字指纹后的 Lena 图像分别进行如下退化处理:高斯噪声、椒盐噪声、剪切、JPEG 压缩和中值滤波等.分别从退化处理后的 Lena 图像中提取指纹,然后用基于协同学的指纹匹配算法进行模式匹配,识别指纹.实验结果见表 2.表 2 第 4 列的序参量演化图中最上方的曲线表示数字指纹  相应序参量的演化过程,即数字指纹  的匹配过程.

Table 1 Robustness test in LSB domain

表 1 LSB 域鲁棒性实验

Image degradation process	Lena after some treatment	Fingerprints extracted	Order parameter curves	Results
Gaussian noise				Fail
Salt and pepper noise				Succeed
Cut 1				Succeed
Cut 2				Fail
Median filtering				Succeed

(a) Digital fingerprint extracted
(a) 提取的数字指纹



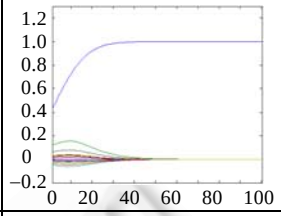
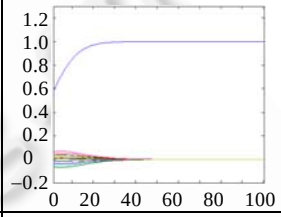
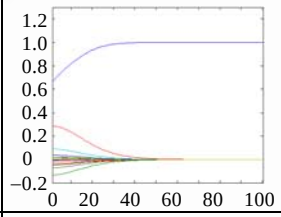
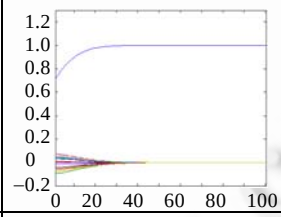
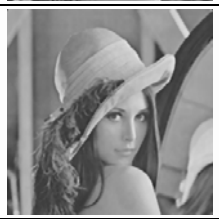
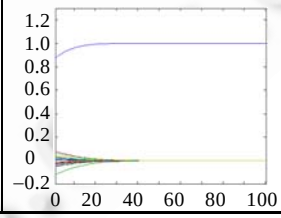
(b) Order parameter evolution curves
(b) 序参量演化图

Fig.8 Digital fingerprint and order parameter evolution curves in DCT domain

图 8 DCT 域的数字指纹及对应的序参量演化图

Table 2 Robustness test in DCT domain

表 2 DCT 域鲁棒性实验

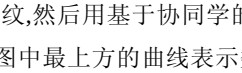
Image degradation process	Lena after some treatment	Fingerprints extracted	Order parameter curves	Results
Gaussian noise				Succeed
Salt and pepper noise				Succeed
Cut				Succeed
JPEG compression				Succeed
Median filtering				Succeed

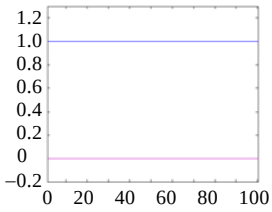
从表 2 中结果可以看出,经过高斯噪声、椒盐噪声、剪切、JPEG 压缩和中值滤波退化操作后,提取出的数字指纹仍然成功匹配.特别是在高斯噪声、椒盐噪声和 JPEG 压缩攻击后,提取出的数字指纹在视觉上已经很难辨认了.但是从序参量演化图中可以看出,匹配过程迅速而准确地完成.

(3) DWT 域

实验中,整数小波变换 DWT 算法借鉴文献[11]的嵌入算法.实验以原始 Lena 图像作为载体图像,嵌入数字指纹 ,得到含指纹信息的 Lena 图像.

对含有数字指纹的 Lena 图像不作任何处理,提取指纹得到数字指纹及其序参量演化图,如图 9 所示.

对嵌入数字指纹后的 Lena 图像分别作如下退化处理:高斯噪声、椒盐噪声、剪切、JPEG 压缩和中值滤波 5 种.分别在退化处理后的 Lena 图像中提取指纹,然后用基于协同学的数字指纹匹配方法进行模式匹配,识别指纹.实验结果见表 3.表 3 第 4 列的序参量演化图中最上方的曲线表示数字指纹  的匹配过程.



(a) Digital fingerprint extracted
(a) 提取的数字指纹

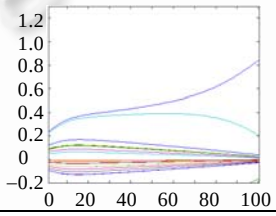
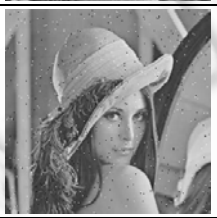
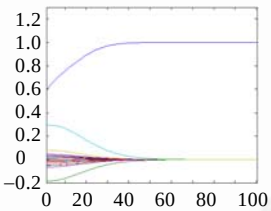
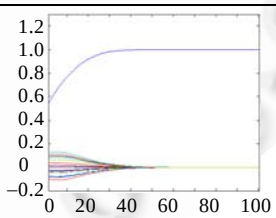
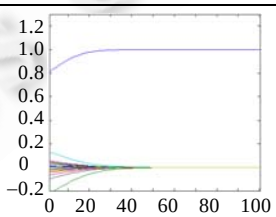
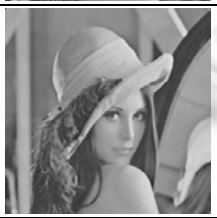
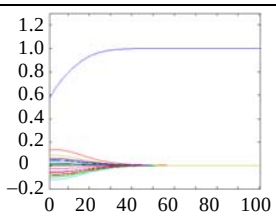
(b) Order parameter evolution curves
(b) 序参量演化图

Fig.9 Digital fingerprint and order parameter evolution curves in DWT domain

图 9 DWT 域的数字指纹及对应的序参量演化图

Table 3 Robustness test in DWT domain

表 3 DWT 域鲁棒性实验

Image degradation process	Lena after some treatment	Fingerprints extracted	Order parameter curves	Results
Gaussian noise				Succeed
Salt and pepper noise				Succeed
Cut				Succeed
JPEG compression				Succeed
Median filtering				Succeed

从表 3 中结果可以看出,经过多种退化操作后,数字指纹仍然成功匹配.即使是在高斯噪声、剪切和中值滤波攻击后,提取出的数字指纹在视觉上看来破坏相当严重.但是从序参量演化图中可以看出,除高斯噪声操作外,其他几种退化操作后的匹配过程在较短步数后都成功匹配.高斯噪声退化处理的序参量演化图与其他几种操作相比,所花费时间较多些,但仍匹配成功.

3.2 抗合谋实验

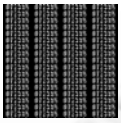
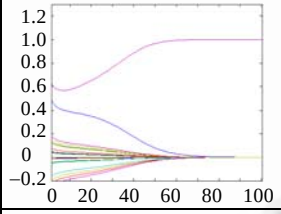
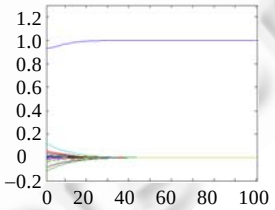
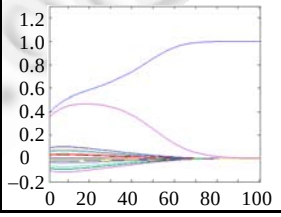
(1) 合谋篡改攻击

实验中,用户 *A* 和 *E* 分别向媒体提供商 SP 购买了 Lena 图像,SP 分别在他们购买的作品中嵌入指纹 012345 和 072319.

A 和 *E* 通过比较两幅作品不同之处确定嵌入指纹的位置,试图通过篡改来抹去指纹.表 4 记录了在 LSB, DCT 和 DWT 嵌入算法下,本方案对合谋篡改攻击的跟踪情况.在表 4 第 5 列的序参量演化图中,LSB 行图中上方第 2 条曲线以及 DCT 行和 DWT 行图中上方第 1 条曲线表示数字指纹 012345 的匹配过程;LSB 行图中上方第 1 条曲线、DCT 行图中上方第 3 条曲线和 DWT 行图中上方第 2 条曲线表示数字指纹 072319 的匹配过程.其中,LSB 和 DCT 域的篡改定位图为原图大小的缩小显示.

Table 4 Collusion-Tampering attack tracking

表 4 合谋篡改攻击跟踪

Embedding domain	Fingerprint	Lena after tampering	Fingerprint extracted	Order parameter curves	Results
LSB					Succeed
DCT					Succeed
DWT					Succeed

由于嵌入前的置乱预处理等手段,合谋篡改攻击往往取得的攻击效果并不好,由表 4 中可以看出,受攻击后提取的指纹有些部分没有被篡改,残留特征较多,比较容易识别与跟踪.表中 LSB 域、DCT 域和 DWT 域都成功地识别了跟踪.

(2) 合谋平均攻击

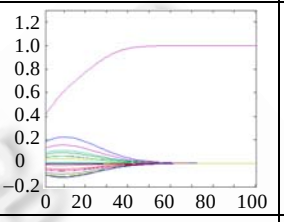
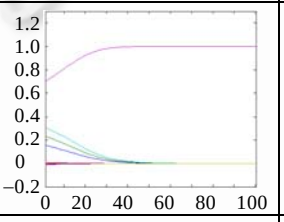
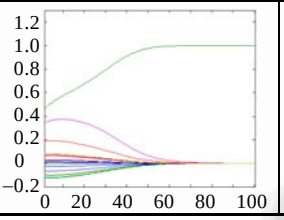
实验中,用户 *A*~*E* 分别向媒体提供商 SP 购买了 Lena 图像.SP 分别在他们购买的作品中嵌入指纹 012345, 012348, 812345, 012848 和 072319.

A,*B*,*D*,*E* 合谋平均攻击,他们把分别购买的合法作品求和平均,试图抹去数字指纹.表 5 记录了 LSB,DCT 和

DWT 嵌入算法下,本方案对合谋篡改攻击的跟踪情况.在表 5 第 4 列的序参量曲线中,LSB 行图中上方第 2 条曲线和 DCT 行图中上方第 4 条曲线表示数字指纹012345的匹配过程;LSB 行和 DCT 行图中上方第 1 条曲线以及 DWT 行图中上方第 2 条曲线表示数字指纹072319的匹配过程;LSB 行图中上方第 4 条曲线、DCT 行图中上方第 3 条曲线和 DWT 行图中上方第 1 条曲线表示数字指纹012348的匹配过程.

Table 5 Collusion-Average attack tracking

表 5 合谋平均攻击跟踪

Embedding domain	Lena after average attack	Fingerprint extracted	Order parameter curves	Results
LSB				Succeed
DCT				Succeed
DWT				Succeed

从表 5 中可以看出,LSB 域、DCT 域和 DWT 域的合谋平均攻击对水印破坏程度较高.在平均攻击中,多用户参与其中,序参量演化后成功跟踪到一个合谋者,被成功跟踪的数字指纹序参量最后演化为 1,而与该曲线最靠近的序参量代表的用户可能是合谋的参与者.

3.3 实验结果分析

鲁棒性实验结果表明,在 LSB 域中嵌入数字指纹时,数字指纹的鲁棒性得不到保证.除了椒盐噪声以外的情况下,数字指纹的匹配发生的错误的概率都很大.但这主要是因为在 LSB 域嵌入指纹的鲁棒性太差而造成的.在 DCT 域中和 DWT 域中嵌入数字指纹,通常可以以非常高的概率正确地进行数字指纹的匹配,即使数字指纹已经遭受到很大程度的破坏.实验表明,在 DCT 域和 DWT 域中,本文提出的数字指纹匹配算法有很好的性能.

抗合谋实验结果表明,在本文提出的方案中,LSB 域、DCT 域和 DWT 域中嵌入数字指纹遭受到合谋攻击,无论是合谋篡改攻击还是平均攻击,都能够以较大的概率成功跟踪到非法用户,这表明本文提出的基于残留指纹特征跟踪的数字指纹抗合谋的思想和方案是可行的.

在保证了正确跟踪的成功率的同时,该指纹方案与基于组合论的数字指纹方案相比,在系统性能方面还具有如下优点:

(1) 编码的效率高.数字指纹可以为有意义的图像,方便了用户和发行商.固有的数字指纹方案都是靠编码来保证抗合谋特性,将用户信息编码为无意义的 0 和 1 序列.有意义的数字指纹可以方便发行商追踪非法用户,在数字指纹损坏程度不大的情况下,可以直接辨认数字指纹,省去了数字指纹的匹配和跟踪过

程.同时,在本文的方案中,码长每增加 55 位,可容纳的用户数就增加 10 倍,编码的效率比基于组合论的编码(如 I 码、C 安全码和 BIBD 码)都要高得多.

(2) 跟踪算法效率高.当前,基于组合论编码的数字指纹方案的跟踪算法要求在大小至少为 $C_n^1+C_n^2+C_n^3+...+C_n^N$ (n 为用户数,N 为抵抗合谋攻击的最大合谋用户数)的模式库中运行匹配算法,而本文提出的基于协同学的数字指纹跟踪方案中,模式库大小只需为 n.

(3) 至少可以成功跟踪到 1 个合谋者,序参量演化曲线可以作为参考来确定其他合谋嫌疑人.被成功跟踪的数字指纹序参量最后演化为 1,而与该曲线最靠近的序参量代表的用户可能是合谋的参与者.

4 结 语

本文提出了基于残留特征跟踪的数字指纹思想,并基于该思想给出了一种线性无关特征码及其数学描述和性质,提出了一种线性无关特征码的数字指纹生成方法;在线性无关特征码的生成方法和基于协同学的数字指纹匹配方法的基础上,提出了基于残留特征跟踪的数字指纹方案.大量实验及分析结果表明,该方案可以提供很好的数字指纹鲁棒性和合谋容忍性;同时,该方案的编码效率和指纹跟踪效率都比基于组合论的数字指纹要高得多.同时,实验结果表明有许多问题尚未解决.该抗合谋思想还需要更多的实验进行验证,还存在不能正确匹配和跟踪的情况.线性无关特征码的特征阈值α和特征差阈值β的确定,这是需要大量实验才能确定的.只有这两个阈值确定是合理的,它们才能指导生成合理的数字指纹库,才能保证合谋产生的新模式不会与已有指纹模式更匹配,才能保证基于残留特征的数字指纹跟踪成功.

References:

[1] Voloshynovskiy S, Pereira S, Iquise V, Pun T. Attack modelling towards a second generation watermarking benchmark. Signal Processing, 2001,81(6):1177−1214. [doi: 10.1016/S0165-1684(01)00039-1]

[2] Fernandez M, Sorano M. Identification of traitors in algebraic-geometric traceability codes. IEEE Trans. on Signal Processing, 2004,52(10):3073−3077. [doi: 10.1109/TSP.2004.833858]

[3] Wu M, Trappe W, Wang ZJ, Liu KJR. Collusion-Resistant fingerprinting for multimedia. In: Katsaggelos AK, ed. Proc. of the IEEE Int'l Conf. on Acoustics, Speech, and Signal Processing (ICASSP 2002). Orlando: Institute of Electrical and Electronics Engineers Inc., 2002. 3309−3312. [doi: 10.1109/MSP.2004.1276103]

[4] Barg A, Blakley GR, Kabatiansky GA. Digital fingerprinting codes: Problem statements, constructions, identification of traitors. IEEE Trans. on Information Theory, 2003,49(4):852−865. [doi: 10.1109/TIT.2003.809570]

[5] Trappe W, Wu M, Wang ZJ, Liu KJR. Anti-Collusion fingerprinting for multimedia. IEEE Trans. on Signal Processing, 2003,51(4): 1069−1087. [doi: 10.1109/TSP.2003.809378]

[6] Huang WJ, Yao J, Guo L. A collusion secure fingerprinting scheme based on nonlinear combinatorial code. Computer Engineering and Applications, 2004,40(24):145−148 (in Chinese with English abstract).

[7] Zhu Y, Yang YT, Feng DG. Convolutional fingerprinting information codes for collusion security. Journal of Software, 2006,17(7): 1617−1626 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/17/1617.htm [doi: 10.1360/jos171617]

[8] Haken H. Synergetic Computers and Cognition—A Top-Down Approach to Neural Nets. Berlin: Springer-Verlag, 1991.

[9] Friedman GL. The trustworthy digital camera: Restoring credibility to the photographic image. IEEE Trans. on Consumer Electronics, 1993,39(4):905−910. [doi: 10.1109/30.267415]

[10] Cox IJ, Kilian J, Leighton FT, Shamoon T. Secure spread spectrum watermarking for multimedia. IEEE Trans. on Image Processing, 1997,6(12):1673−1687. [doi: 10.1109/83.650120]

[11] Zhu Q, Zhu GX, Li N. Digital watermarking technique for grayscale images based on integer wavelet transform. Computer Engineering and Applications, 2004,40(6):54−56,62 (in Chinese with English abstract).

[12] Wang ZX, Ge Q, Wang WZ, Hu HP. Digital fingerprinting based on Synergetic. In: Romeo D, ed. Proc. of the Int'l Conf. on Computational Intelligence and Software Engineering (CiSE 2009). Piscataway: IEEE Computer Society, 2009. 1−4. [doi: 10.1109/CISE.2009.5365218]

附中文参考文献:

[6] 黄万钧,姚俊,郭雷.一种基于非线性组合编码的安全指纹方案.计算机工程与应用,2004,40(24):145−148.

[7] 朱岩,杨永田,冯登国.合谋安全的卷积指纹信息码.软件学报,2006,17(7):1617−1626. http://www.jos.org.cn/1000-9825/17/1617.htm [doi: 10.1360/jos171617]

[11] 宋琪,朱光喜,李宁.基于整数小波变换的灰度图像水印技术.计算机工程与应用,2004,40(6):54−56,62.

王祖喜(1964－),男,湖北武汉人,博士,副教授,主要研究领域为网络信息安全,模式识别与智能系统,数字水印,数字版权保护.

葛强(1982－),男,硕士,主要研究领域为网络与信息安全.

王文宗(1984－),男,硕士,主要研究领域为网络与信息安全.

胡汉平(1960－),男,博士,教授,博士生导师,主要研究领域为网络与信息安全.