一种基于频分复用的数字指纹技术

晏钊韬，张汗灵
（湖南大学计算机与通信学院，长沙 410082）

摘 要：传统的数字指纹编码方案由于其自身存在性问题和相关检测的复杂性，使其指纹的生成效率和跟踪效率很低。针对上述问题，提出了一种新的基于频分复用的数字指纹编码方案。该方案以频谱不相互重叠的余弦信号的抽样作为数字指纹，通过扩频序列将指纹嵌入到原始图像的中频系数中。同时结合嵌入算法分析了其抗合谋性能，并从理论上推导出码字长度与用户人数之间的关系。仿真实验表明了该方案的可行性和有效性。

关键词：数字指纹；版权保护；频分复用；傅里叶变换
中图法分类号：TP309 **文献标志码**：A **文章编号**：1006-8961(2010)09-1326-05

Digital fingerprint scheme based on the FDM-technique

YAN Zhaotao, ZHANG Hanling
(*School of Computer and Communications, Hunan University, Changsha* 410082)

Abstract: Due to the existence problem and complexity on correlative detection, traditional digital fingerprinting schemes have low efficiency in construction and tracking. To solve this problem, a new fingerprinting scheme based on the FDM (frequency division multiplexing) technique is proposed in this paper. In this scheme, the digital fingerprinting, which is a random sample from Cosine signal with no spectral overlap, is embedded in the middle-frequency coefficients of the original image through the spreading sequences. The performance of anti-collusion by embedding algorithm is also analyzed so as to theoretically deduce the relationship between code length and user size. The experimental results demonstrate the feasibility and efficiency of the scheme.

Keywords: digital fingerprinting; copyright protection; FDM; Fourier transform

0 引 言

随着信息技术和互联网的迅猛发展，数字多媒体（音频，图像，视频）与用户的联系越来越紧密，用户能够轻松地访问它们。然而，这种便利性也引起了一个严重的问题，即多媒体资源的随意编辑、修改、拷贝和散布，它严重地威胁到了数字作品的版权保护和信息安全。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。发行商通过在其所要发售的拷贝中嵌入与购买者有关的数字指纹，对盗版行为进行跟踪，以达到保护发行者版权利益的目的。

数字指纹编码作为数字指纹技术的核心，其目的是要抵抗合谋攻击。Trappe 等人以均衡不完全区组设计为基础提出了一种 BIBD 码[1]，然而在某参数下 BIBD 设计本身的存在性及相应的 BIBD 区组的获取都存在问题，在参数比较大的情况下，寻找 BIBD 区组的算法是相当复杂的。Cox 等人采用独立随机的正态采样序列作为数字指纹[2]，该方法构造简单，但在用户比较多的情况下，其跟踪算法的计算量大。

针对以上问题，运用频分复用的思想，提出了一种具有良好指纹生成效率和跟踪效率的新的数字指纹编码方案。结合嵌入算法，分析了其抗合谋攻击的性能，并从理论上推导了码字长度与用户人数之

基金项目：湖南省自然科学基金(08JJ4019)；长沙市科技计划(k0803106-11)；国家重点基础研究发展计划(973)项目(2006CB303000)。
收稿日期：2009-01-07；**改回日期**：2009-05-05

第一作者简介：晏钊韬(1984—)，男。湖南大学计算机与通信学院信息与通信工程硕士研究生。主要研究方向为图像处理与数字水印。E-mail: Zhang_hl2002@ hotmail. com。

间的关系。

1　数字指纹系统

数字指纹系统主要由两部分构成,一是用于向拷贝中嵌入指纹并对带指纹拷贝进行分发的拷贝分发子系统;另一部分是实现对非法分发者进行跟踪并审判的跟踪子系统。其中分发子系统完成指纹的构造、指纹的嵌入以及数据库的维护工作,跟踪子系统完成指纹的提取和跟踪工作[3]。其简单模型见图 1。

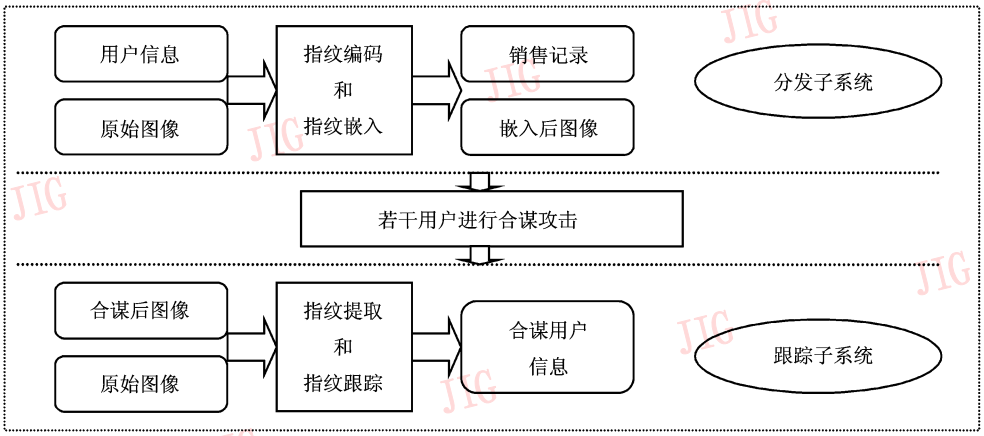


图 1　数字指纹系统简单模型

Fig. 1　Simple model of digital fingerprint system

指纹编码算法的作用主要是抵抗合谋攻击[4]。合谋攻击是几个盗版者联合起来,通过对各自的拷贝进行比较,定位出部分标记的位置。然后综合所有原始数据拷贝制造出一个新的数据拷贝,从而使新拷贝中提取出的指纹是一个无效的指纹(不能指示任何用户)或是无辜用户的指纹。

指纹的嵌入算法主要用于抵抗对指纹的稳健性攻击[5],包括有意攻击和无意攻击两大类。嵌入算法有不可见性和对单用户攻击的鲁棒性要求,这一点与狭义数字水印(用于标识版权的数字水印)的嵌入算法相同,可以直接采用数字水印的嵌入算法。

指纹的提取算法可以看做是指纹嵌入算法的逆过程。而对于指纹的跟踪算法,能够成功地跟踪出一个合谋者,则该跟踪算法是成功的;如果没有识别出任何一个合谋者或者是将一个无辜用户指证为合谋者,则认为该跟踪算法是失败的。

2　分发子系统

2.1　指纹构造

以信号强度为 E,时长为 τ 的矩形信号作为初始信号,用不同频率 $w \in \{w_1, w_2, \cdots, w_N\}$ 的余弦信号与初始信号进行相乘,并用抽样频率 f_s 对所得信号进行抽样,得到 N 个长度为 L 的抽样信号 $\boldsymbol{M} = (m_1, m_2, \cdots, m_L)$。$\boldsymbol{M}$ 即为用户的指纹。N 为用户人数,$L = f_s \times \tau$ 为指纹码长。当抽样频率 f_s,信号强度 E,时长 τ 一定的时候,用户的指纹由用户频率 w_i 唯一的确定。

2.2　指纹嵌入

本文使用变换域方法,即先对图像作某种变换,然后通过改变变换系数来加入指纹。嵌入步骤为

1) 对原始图像做全局的离散余弦变换(DCT);

2) 用密钥 Z_1 从变换系数中选取 L 个中频系数 $\boldsymbol{V} = (v_1, v_2, \cdots, v_L)$;

3) 用密钥 Z_2 产生长度为 L 的由 ±1 构成的伪随机序列 $\boldsymbol{P}$。

4) 生成扩频后的指纹 $\boldsymbol{M}' = \boldsymbol{M} \cdot \boldsymbol{P}$;

5) 把扩频指纹 $\boldsymbol{M}'$嵌入到这 L 个中频系数中,采用式:$v_i' = v_i + \alpha m_i'$。其中 m'为第 i 位扩频指纹,α 为嵌入强度,v_i' 为嵌入指纹后的系数;

6) 进行反离散余弦变换(IDCT),得到嵌入指纹后的图像。

2.3　抗合谋性能分析

合谋攻击可分为以平均攻击为代表的线性攻击和以最小值最大值为代表的非线性攻击。其数学形式可用式(1)表示[6]

$$v_c = v + h^{-1}\left(\psi\left(h(M_1), h(M_2), \cdots, h(M_k)\right)\right) \quad (1)$$

式中,K 为合谋人数,v 为图像载体,v_c 为攻击后的共

谋图像，ψ 为合谋攻击函数，$M_1, M_2, \cdots, M_k$ 为参与合谋的用户指纹，h 为嵌入域变换到攻击域的函数，相应地，h^{-1} 为攻击域变换到嵌入域的函数[6]。而攻击者对于函数 h 是一无所知的，因此，攻击者一般是在空域进行合谋攻击。

对于线性平均攻击，其形式为

$$M_{ave} = \frac{M_1 + M_2 + \cdots + M_K}{K} \tag{2}$$

根据傅里叶变换的性质[7]，相加信号的频谱等于各个单独信号的频谱之和。因此当用户指纹的频谱不相互重叠的时候，该方案能够有效地抵抗线性平均攻击。而对于非线性攻击，文献[6]指出，如果不在指纹的嵌入域进行攻击，则非线性的合谋攻击效果将会显著降低，与平均攻击的效果基本相当。因此，当合理选择参数的情况下，该方案具有良好的抗合谋性能。

2.4 指纹码长

初始信号与频率为 w_0 的余弦信号在时域相乘，初始信号的中心频率将被搬移到载频 $\pm w_0$ 处。如式(3)所示

$$\Im[f(t)] = \Im[g(t)\cos(w_o t)] = F(w) = \frac{1}{2}[G(w + w_o) + G(w - w_o)] \tag{3}$$

式中，$\Im$ 为傅里叶变换，$f(t)$ 为已调信号，$F(w)$ 为已调信号的频谱，$g(t)$ 为初始信号，$G(w)$ 为初始信号的频谱。

当用户进行平均攻击后，为了进行叛逆者追踪，应使信号频谱不相互重叠，即

$$w_{i+1} - w_i \geqslant B \tag{4}$$

B 为初始信号的频宽。而信号强度为 E，时长为 τ 的矩形信号，其频宽为 $4\pi/\tau$。

根据抽样定理[7]，抽样角频率 w_s 应大于已调信号的最大频宽 B_{max}。从式(3)和式(4)可得：

$$B_{max} \geqslant 2NB = 2N\frac{4\pi}{\tau} \tag{5}$$

又 $w_s = 2\pi f_s$，$L = f_s\tau$，可得到 $L \geqslant 4N$。式(5)表明，当用户人数为 N 时，需要使用 $4N$ 的码字长度。

3 跟踪子系统

3.1 指纹提取与跟踪

使用原始图像并已知密钥 Z_1 和 Z_2 来对指纹进行提取和跟踪。对于用户 i，因嵌入的指纹实际为有限余弦信号的抽样，其频谱 $F(w)$ 在用户频率 w_i 处会有一峰值。因此能通过阈值找出一个或几个合谋用户。提出和跟踪步骤：

1）对原始图像和检测图像做全局 DCT 变换；

2）用密钥 Z_1 提出系数 $\boldsymbol{V} = (v_1, v_2, \cdots, v_L)$ 和 $\boldsymbol{V}'' = (v_1'', v_2'', \cdots, v_L'')$。$V''$为攻击后系数；

3）通过式 $m_i'' = (v_i'' - v_i)/\alpha$，得到攻击后的扩频指纹 $M'' = (m_1'', m_2'', \cdots, m_L'')$；

4）使用密钥 Z_2 产生伪随机序列 $\boldsymbol{P}$；

5）得到合谋攻击后的指纹 $\hat{\boldsymbol{M}} = \boldsymbol{M}'' \cdot \boldsymbol{P}$；

6）求 $\hat{\boldsymbol{M}}$ 的频谱 $F(w)$，选取门限 T，如果 $F(w_i) > T$，则判定用户 i 为合谋者。

3.2 合谋人数估计与门限选取

合谋人数是门限选取的一个重要依据。现考虑式(2)所示的平均攻击，当指纹参数确定了的情况下，$\hat{\boldsymbol{M}}$ 的频谱幅度随着合谋人数的增加而线性减少。因此可以通过频谱幅度来确定合谋人数。然而在实际情况下，合谋者的频谱幅度不是均匀分布的。因此采用频谱幅度的最大值来估计合谋人数，其表达式为

$$K = \frac{F}{F(w)_{max}} \tag{6}$$

式中，F 为嵌入指纹的原始频谱幅值，根据傅里叶变换和抽样定理的性质，其取值为 $E\tau f_s/2$，$F(w)_{max}$ 为 $\hat{\boldsymbol{M}}$ 频谱的最大值。为了在跟踪算法中追踪到至少一个合谋用户，门限可以选择 $T = F/(K+1)$。因为合谋人数 K 是使用式(6)估算出来的，$F(w)_{max}$ 永远大于 T，满足至少跟踪到一个合谋用户的要求。并且当合谋者的频谱幅度越趋向于均匀，能追踪到的合谋用户越多。

4 实验结果

在 Matlab 平台上进行了仿真实验，宿主图像为 512×512 的 Lena 灰度图像。采用信号强度为 1，时长为 4π 的矩形信号作为初始信号，用户角频率间隔为 1，它满足上述所说的要求。抽样频率 f_s = 1 000，嵌入强度为 10。

图 2 给出了原始图像与嵌入指纹后图像的对比结果。嵌入指纹后，图像的信噪比在 37.7 左右，满足不可见性的要求。表 1 为使用跟踪算法得到的结果。图 3 给出了各种攻击情况下提取出指纹后所对应的傅里叶变换结果。

(a) 原始图像　　(b) 嵌入后图像

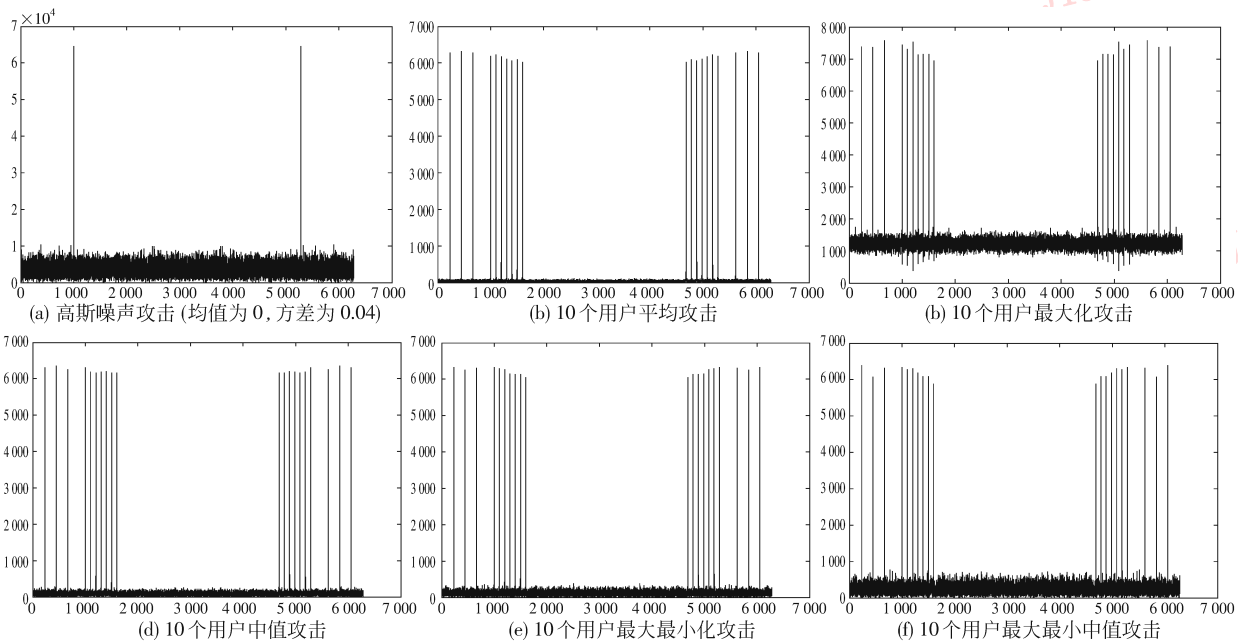
图 2　原始图像和加入指纹后的图像

Fig. 2　The original image and the image embedded fingerprinting

表 1　跟踪结果

Tab. 1　Results of tracking

合谋人数	攻击方式	合谋人数估计	追踪人数
1	噪声攻击	1	1
10	平均攻击	10	10
10	最大化攻击	8	9
10	最小化攻击	12	10
10	中值攻击	10	10
10	最大最小化攻击	10	10
10	最大最小中值攻击	10	10



(a) 高斯噪声攻击 (均值为 0, 方差为 0.04)　(b) 10 个用户平均攻击　(b) 10 个用户最大化攻击

(d) 10 个用户中值攻击　(e) 10 个用户最大最小化攻击　(f) 10 个用户最大最小中值攻击

图 3　各种攻击下指纹的傅里叶变换结果比较

Fig. 3　Comparison of Fourier transform results of fingerprinting under different attacks

从图 3 和表 1 可以看出,因用户指纹的频谱不相互重叠,平均攻击后指纹频谱不会相互影响,其跟踪效果最好,因此能够抵抗大量用户的平均攻击。而对于中值攻击等非线性攻击,因不在指纹的嵌入域进行攻击,其效果与平均攻击基本相当。其中,虽然最大化攻击或最小化攻击后对合谋人数估计有些许误差,但仍然能有效和正确地追踪到部分合谋用户。

5　结　论

提出了一种新的基于频分复用的数字指纹编码方案。与其他指纹编码方案相比[8-9],该方案构造简单,同时对于不同用户,只需存储不同用户频率 w_i,减少了指纹的存储空间。在指纹跟踪方面,因不需要与所有用户指纹做相关性检测,减少了其计算复杂度,提高了跟踪效率。理论和实验表明,该方案具有良好的抗合谋攻击性。

参考文献(References)

[1] Trappe W, Wu M, Liu K R. Collusion-resistant fingerpringting for multimedia[J]. IEEE Signal Processing Magazine, 2004, 21(2): 15-27.

[2] Cox I J, Kilian J. Secure spread spectrum watermarking for

multimedia[J]. IEEE Transactions on Image Processing, 1997, 6(12): 1673-1687.

[3] LV Shuwan, Wang Yan, Liu Zhenhua. A survey of digital fingerpring[J]. Journal of the Graduate School of the Chinese Academy of Science, 2004, 21(3): 289-298.[吕述望, 王彦, 刘振华. 数字指纹综述[J]. 中国科学院研究生院学报, 2004, 21(3): 289-298.]

[4] Wu M, Wang Z J. Forensic analysis of nonlinear collusion attacks for multimedia fingerprinting[J]. IEEE Transactions on Image Processing, 2005, 14(5): 646-661.

[5] Wang Zhixiong, Wang Huiqin. Attacks and remdies on application of digital watermarking[J]. Journal of China Institute of Communications, 2002, 23(11): 74-79.[王志雄, 王慧琴. 数字水印应用中的攻击和对策综述[J]. 通信学报, 2002, 23(11): 74-79.]

[6] Chen Zhenyong, Xiong Zhang. Method against nonlinear collusion attack for digital fingerpringting[J]. Journal of Harbin Institute of Technology, 2006: 830-833.[陈真勇, 熊璋. 数字指纹的非线性共谋攻击抵抗方法[J]. 哈尔滨工业大学学报, 2006: 830-833.]

[7] Zheng Junli, Yang Weili. Signals and Systems(second edition)[M]. Beijing: Higher Education Press, 2000.[郑君里, 杨为里. 信号与系统(第二版)[M]. 北京: 高等教育出版社, 2000.]

[8] Wu M, Wade T, Wang Z J. Anti-collusion Forensics of Multimedia fingerprinting using orthogonal modulation[J]. IEEE Transactions on Image Processing, 2005, 14(6): 804-821.

[9] Dan B, Janes S. Collusion-secure fingerprinting for digital data[J]. IEEE Transactions on Information Theory, 1995, 44(5): 1897-1905.