一种基于树结构的高斯分布扩频指纹嵌入技术的方法研究*

赵慧民，张惠乐，胡学骏
（佛山科学技术学院机电学院，广东 佛山 528000）

摘 要：数字指纹是目前保护多媒体内容不受非法拷贝分配的最新技术。一定条件下，多媒体拷贝内容能够有效跟踪非法用户并抗击共谋攻击是其应用的关键技术。在多播环境下，考虑带宽影响研究了一种基于树结构的扩频指纹嵌入系统。该系统在高斯分布情况下，对一定的共谋攻击者，系统俘获其的概率比正交扩频指纹系统提高了约 40%，从而增强了追踪非法用户的能力，进一步提高了指纹加密系统的鲁棒性。

关键词：树结构；扩频；高斯分布；指纹系统；多媒体视频流
中图分类号：TN918 文献标识码：A 文章编号：0529-6579（2006）01-0042-04

目前信息技术的发展使 Internet上多媒体分配和共享成为现实。为了保证多媒体内容的合法分配和正确使用，多媒体指纹系统主要考虑两种情况。首先是共谋攻击篡改，即几个用户公用几个相同内容的内容拷贝但嵌入不同的指纹。第二是网络上大量数据需要传输到多用户时的多媒体视频流应用系统。本文考虑传输带宽的影响主要研究第二种情况的安全机制。

为了抗共谋攻击，数字指纹在多媒体视频流的嵌入主要有两种算法：扩频指纹系统和高斯指纹系统[1]。扩频指纹系统隐藏和提取信息操作复杂，适合于数字作品版权保护；高斯指纹系统由于抗共谋攻击和用户是函数关系[2]，当用户很多时，用于估计某一用户的计算量太大，所以，其在多播系统中应用有限。文献 [3] 提出一种指纹嵌入和解密集成的方案，该方法对检测器有一定的特别要求。根据文献 [4－6] 的结果，在多播传输环境下，考虑带宽的限制，本文基于树结构提出了一种扩频指纹调制嵌入系统。

1 多媒体视频流加密的要求

在视频流应用中，为了保护知识产权和内容拥有者的利益，合理分配并管理多媒体内容是目前网络设计的技术热点。视频流应用加密的要求是：

（1）视频内容加密：仅仅允许和内容服务商登记的合法用户可以访问视频内容。

（2）非法用户跟踪：数据分配到合法用户后，内容服务提供者必须保护多媒体内容不被再分配。而数字指纹是跟踪非法用户的一种有效手段，并且其可以用来识别盗版拷贝的根源所在。

（3）嵌入指纹的鲁棒性：如果应用了数字指纹嵌入技术，那么需要嵌入的指纹能支持常用的信号处理（如有损压缩），攻击以及多用户共谋攻击。

（4）反帧攻击技术：公开的文本内容只有相应嵌入自己指纹的那些合法用户已知，其他用户无权访问并对内部用户进行帧篡改估计攻击。

2 基于树结构的扩频指纹嵌入和分配机制

根据扩频和高斯指纹嵌入在多播环境的不同[4－6]，为了进一步利用有效带宽，这里提出一种基于树结构的扩频指纹嵌入设计和分配机制。它利用了在高斯分布下扩频调制方法进行嵌入指纹信息，同时考虑了传输带宽和系统抵抗共谋攻击因素的影响。

2.1 基于树结构的扩频指纹调制方法

基于树结构的指纹设计如图 1所示。其唯一的指纹向量 $a^{i_1,\cdots,i_l}$在树节点 $[i_1, \cdots, i_l]$ 上按照高斯分布 $N(0, \sigma_w^2)$ 产生，其中 l是节点的深度，而 i是某个用户节点，同时指纹向量集 $\{a\}$ 相互独立。对于用户 $u^{(i)}$其索引是 $i=[i_1, i_2, \cdots, i_l]$。分配给 $u^{(i)}$的指纹拷贝 $X^{(i)}$中，总的嵌入的 L 个指纹是 a^{i_1}，a^{i_1,i_2}，$\cdots$，$a^{i_1,\cdots,i_L}$。假设主机信号 S 有 N 个可能嵌入的指纹系数，那么嵌入 L 个指纹到 S 中

* 收稿日期：2005－05－11
基金项目：广东省自然科学基金资助项目（04105503）；佛山市科技发展专项基金资助项目（04010052）
作者简介：赵慧民（1966年生），男，博士，副教授；E-mail: zhaohuimin@tom.com

有两种不同的方法：基于扩频和基于正交扩频指纹调制技术。以下研究两种方法在基于树结构的不同应用情况。

(1) 基于扩频的指纹调制方法：在常用扩频的指纹调制中，指纹向量集 $\{a\}$ 有相同的长度 N 和等价的容量。用户 $u^{(i)}$ 的指纹 $W^{(i)}$ 通过下式产生：

$$W^{(i)} = \sqrt{\rho_1}a^{i_1} + \sqrt{\rho_2}a^{i_1,i_2} + \cdots + \sqrt{\rho_L}a^{i_1,i_2,\cdots,i_L} \tag{1}$$

那么，分配给 $u^{(i)}$ 的指纹拷贝为：

$$X^{(i)} = S + W^{(i)} \tag{2}$$

其中，$\{\rho_l\}$ 表示共谋攻击时不同分支树情况下用户数的概率，且有 $0 \leqslant \rho_1, \cdots \rho_L \leqslant 1$，$\sum_{j=1}^{L}\rho_j = 1$ 的关系。$\{\rho_l\}$ 用于控制每一级树嵌入指纹的容量并调整不同用户之间已赋值分配的指纹。

(2) 基于正交扩频的指纹调制方法：在正交扩频指纹调制中，主机信号 S 可以被划分为 L 个互不重叠的部分 S_1，…，S_L，这样在 S_l 中可以嵌入的系数是：

$$N_l = \rho_l N, \text{且满足} \sum_{l=1}^{L} N_l = N \tag{3}$$

在正交扩频指纹调制中，l 级指纹集向量 $\{a^{i_1,\cdots,i_l}\}$ 的长度为 N_l，分配给用户 $u^{(i)}$ 的指纹拷贝内容 $X^{(i)}$ 的指纹向量 $a^{i_1,\cdots,i_l}$ 嵌入到第 l 个主机信号 S_l，且满足 $X_l^{(i)} = S_l + a^{i_1,\cdots,i_l}$。

(3) 两种指纹调制方法的性能比较：为了比较两者在树结构指纹嵌入系统中的性能，这里测试了嵌入到拷贝中不同部分的指纹容量。假设 $X_l^{(i)} = S_l + W_l^{(i)}$ 是用户 $u^{(i)}$ 的第 l 部分指纹拷贝内容，定义 $E_{k,l}$ 为嵌入到 $X_l^{(i)}$ 中 k 级指纹向量 $a^{i_1,\cdots,i_k}$ 的容量，$E_l = \triangleq \sum_{k=1}^{L} E_{k,l}$ 为 $W_l^{(i)}$ 的全部容量。

定义矩阵 P 的 k 行 l 列元素为 $p_{k,l} \triangleq E_{k,l}/E_l$，它表示第 k 级指纹向量 $a^{i_1,\cdots,i_k}$ 容量与 $W_l^{(i)}$ 的容量比率大小。那么，两种指纹调制的的矩阵分别是：

$$P^s = \begin{bmatrix} \rho_1 & \rho_1 & \cdots & \rho_1 \\ \rho_2 & \rho_2 & \cdots & \rho_2 \\ \vdots & \vdots & \ddots & \vdots \\ \rho_L & \rho_L & \cdots & \rho_L \end{bmatrix}_{L\times L}$$

$$\text{和 } P^0 = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}_{L\times L} \tag{4}$$

另外，在基于扩频指纹调制方法中有关系

$$P^s[N_1 \quad N_2 \cdots N_L]^T = N[\rho_1 \quad \rho_2 \cdots \rho_L]^T \tag{5}$$

并满足 $\sum_{l=1}^{L} N_l = N$，这里 N 是能够嵌入到主机信号中总的系数数量。

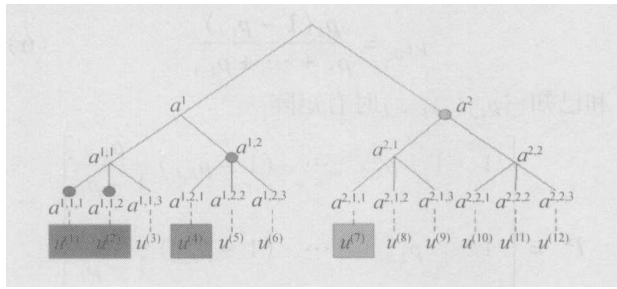

图 1　一种交织共谋攻击时 3级指纹树的结构

Fig. 1　A Structure of the interleaving based collusion attack at level 3 in the fingerprinting tree

假设 SC 是指向共谋攻击的索引设置，$\{X^{(k)}\}_{k\in SC}$ 是他们接收的指纹拷贝内容。在交织共谋攻击时，如果把他们划分成 L 个子集 $SC_l \subseteq SC_{l=1,\cdots,L}$，那么至少存在一个 $1 \leqslant k \leqslant L$ 使第 l 个子组和第 $(l+1)$ 个子组 SC_{l+1} 在树的不同分支上，并且没有重叠，也就是说有 $SC_l \cap SC_{l+1} = \phi$。共谋拷贝 V 包含 L 个互部重叠的部分，且子集中的共谋者通过 $V_l = g(\{X_l^{(i)}\}_{i\in SC_l})$ 产生第 l 个部分共谋拷贝，这里 $g(\cdot)$ 表示共谋攻击函数。

图 1为 3级指纹树设计时，假设 $SC = \{1 = [1, 1, 1], 2 = [1, 1, 2]\}$，$4 = [1, 2, 1]$，$7 = [2, 1, 1]\}$。共谋攻击选择 $SC1 = \{7\}$，$SC2 = \{4\}$ 和 $SC3 = \{1, 2\}$，并产生共谋拷贝 V，其 $V_1 = X_1^{(7)} = S_1 = +a^2$，$V_2 = X_2^{(4)} = S_2 + a^{1,2}$，$V_3 = (X_3^{(1)} + X_3^{(2)})/2 = S_3 + (a^{1,1,1} + a^{1,1,2})/2$。

在检测处理时，树的第一级，虽然 a^1 和 a^2 是非法的，而因为 a^1 并不在 V 中，所以检测器只检测出 a^2 的存在。检测器输出所估计的非法存在域为 $GR(1) = [2]$。在树的第二级，检测器试图检测是否 $[2, 1]$ 和 $[2, 2]$ 是非法子域。但由于 $a^{2,1}$ 和 $a^{2,2}$ 不在 V 中，这两个非法操作都没有被指出。为了继续检测处理，检测器必须检测 V 中 4个指纹 $\{a^{1,i_2}\}$ 的每一个存在指纹。因此，基于正交扩频指纹调制方案的检测处理性能优于常用扩频指纹调制方案的检测性能，这是由于指纹设计的特殊结构及其在树结构多级检测处理时的唯一性造成的。

2.2　树结构高斯分布扩频指纹嵌入的方式

2.2.1　树结构扩频指纹调制的设计　在此提出的指纹调制设计方案，矩阵 P 是一个上三角形方阵。在 P^l 中，为了利用有效带宽，对于 $k > l$ 使 $p_{k,l} = 0$。对于 $k \leqslant l$ 使 $0 < p_{k,l} \leqslant 1$以实现鲁棒性。

在第 1级，$p_{1,1} = 1$。在第 $2 \leqslant k \leqslant L$ 级，已知 p_l，寻找 $\{p_{k,l}\}_{k<l}$ 关系值，满足一种条件为 $E_{1,l}$：$E_{2,l}$，…，$E_{l-1,l} = \rho_1 : \rho_2 : \cdots : \rho_{l-1}$。那么，对

于可 $k<l$有关系：

$$p_{k,l}=\frac{\rho_k(1-p_{l,l})}{\rho_1+\cdots+\rho_{l-1}} \tag{6}$$

和已知 $\{p_{l,l}\}_{l=1,\cdots,L}$时有矩阵

$$P^J=\begin{bmatrix} 1 & 1-p_{2,2} & \cdots & (1-p_{L,L})\dfrac{\rho_1}{1-\rho_L} \\ 1 & p_{2,2} & \cdots & (1-p_{L,L})\dfrac{\rho_2}{1-\rho_L} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & p_{L,L} \end{bmatrix}_{L\times L} \tag{7}$$

在（7）中当 $\sum_{l=1}^{L}N_l=N$，$0\leqslant N\leqslant N$时，寻找 N_1，N_2，…，N_L满足条件

$$P^J[N_1\quad N_2\cdots N_L]^T=N[\rho_1\quad\rho_2\cdots\rho_L]^T \tag{8}$$

在（7）式中，当时 $p_{L,L}=\rho_L$，它就是基于正交扩频指纹调制方法。

2.2.2 树结构扩频指纹调制的指纹嵌入技术 已知（7）式的条件，并且有关系 $N_L=N-\sum_{l=1}^{L}N_l$，那么对于树级 $1<k\leqslant L$的每个指纹向量 $a^{i_1,\cdots,i_l}$有

$$a^{i_1,\cdots,i_l}=a_l^{i_1,\cdots,i_l}\Psi a_{l+1i_1,\cdots,i_l}\Psi a_{Li_1,\cdots,i_l} \tag{9}$$

这里，$\{a_k^{i_1,\cdots,i_l}\}_{k=l,\cdots,L}$按照高斯分布 $N(0,\sigma_W^2)$并相互独立。对于 $k\geqslant l$，长度为 N_k 的指纹向量 $a_k^{i_1,\cdots,i_l}$嵌入到 S_k 中。符号“Ψ”表示了级连因子。对用户 $u^{(i=[i_1,\cdots,i_l])}$，接收到的第 l部分指纹拷贝内容为 $X^{(i_1,\cdots,i_l)}{}_l=S_l+W_l^{(i_1,\cdots,i_l)}$，这里有

$$W_l^{(i_1,\cdots,i_l)}=\sqrt{\rho_{1,l}}a_l^{1i_1}+\sqrt{\rho_{2,l}}a_l^{i_1i_2}+\cdots+\sqrt{\rho_{l,l}}a_l^{i_1,\cdots,i_{l-1}i_l} \tag{10}$$

在检测器端，已知共谋攻击拷贝 V，对于 $1\leqslant k\leqslant L$，检测器从 V_l提取指纹 Y_l。

2.2.3 树结构扩频指纹调制的指纹分配技术 如图 2所示，为 VOD应用中基于 MPEG－2的指纹分配方案。假设 K^m 是所有用户共享的密钥，$K^{(i_1,\cdots,i_l)}$为用户子集 $U^{(i_1,\cdots,i_l)}$共享的密钥。其加密过程类似于文献［3］中指纹多播系统的方式。在指纹嵌入和分配过程中，密钥在服务器端的步骤如下：

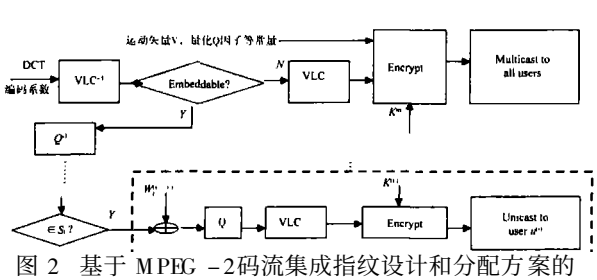

图 2 基于 MPEG－2码流集成指纹设计和分配方案的 VOD应用（服务器端）

Fig. 2 The MPEG－2 based joint fingerprint design and distribution scheme for VOD application (server side)

（1）对于用户 $u^{(i)}$，指纹 $W^{(i)}$按照（10)式产生。

（2）压缩的比特流分成两个部分：第 1部分包含运动矢量，量化因子和其它不变信息；第 2部分，包含 DCT编码系数和可变长解码。

（3）仅改变 DCT系数值，第 1部分的压缩比特流不变。对 DCT系数，如不能嵌入，和其它非嵌入 DCT系数一起进行可变长编码；如果可嵌入，先进行反量化。如果它属于 S_l，对于每个子集 $U^{I_1,\cdots,I_l}=\{u^{(i=[i_1,\cdots,i_l])}:\ j_1=i_1,\ \cdots,\ i_l=j_l\}$，相应地在 $W_l^{I_1,\cdots,I_l}$中使用扩频进行指纹嵌入，嵌入后的指纹系数被量化并和其它在 $X_l^{I_1,\cdots,I_l}$中嵌入的指纹系数进行可变长编码。

（4）非嵌入的 DCT系数用 K^m 加密并多播给所有用户。对于 $1\leqslant l<L$，在 $X_l^{I_1,\cdots,I_l}$中嵌入的指纹系数用 $K^{I_1,\cdots,I_l}$加密并多播给子集 $U^{I_1,\cdots,I_l}$用户。在 $X_L^{(i)}$ 中的指纹系数用用户 $u^{(i)}$的密钥加密并单播给此用户。

3 实验结果与性能分析

为了测试本系统抗击共谋攻击的鲁棒性，假设 $N=10^6$，用户总数 $M=10^4$，P_d 表示至少俘获一个攻击者的概率，P_{fp}表示错误指控一个共谋攻击者的概率。S_A 和 S_B 分别表示 A、B两种不同子集共谋攻击时的索引，并定义合法性参数为 $FP(SC_A,SC_B)\triangleq\dfrac{F_d(SC_A)}{F_d(SC_B)}$，这里 $F_d(SC_A)=\dfrac{\sum_{i\in SC_A}I(i\notin SC)}{|SC_A|}$，$F_d(SC_B)=\dfrac{\sum_{i\in SC_B}I(i\in SC)}{|SC_B|}$

其中 $I[\cdot]$为该系统标识函数，$|SC_A|$和 $|SC_B|$分别表示了 S_A 和 S_B 中共谋攻击者的人数，而 SC 标识了检测器对共谋攻击的估计输出。按照文献［4］设计，简化起见，考虑 $L=4$时，嵌入指纹集向量 $\{a\}$ 的方差按照 $\sigma_W^2=1/9$的高斯 $N(0,\sigma_W^2)$分布对称树结构，且 $[D1,D2,D3,D4]=[4,5,5100]$和 $[\rho_1,\rho_2,\rho_3,\rho_4]=[1/6,1/6,1/6,1/2]$ 在具体实验时，设系统对不同的调制技术有相同的目标比特率，且调制矩阵（7）中 $p_{2,2}=\cdots=p_{L,L}=p=0.95$，$p_{fp}=10^{-2}$。由图 3可见，在共谋攻击者 $K=300$时，该系统俘获其的概率比正交扩频指纹系统提高了 40%。而在图 4中，由于 $FP\ll1$，因此，在子集 SC_L 中的共谋攻击者比在 SC_{L-1}中更容易被检测出来。

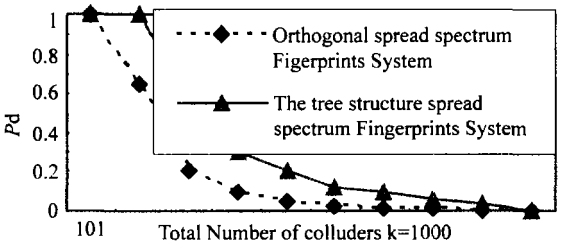

图 3　基于交织共谋攻击的 P_d 性容分析

Fig. 3　P_d per. interleaving based collusion attacks

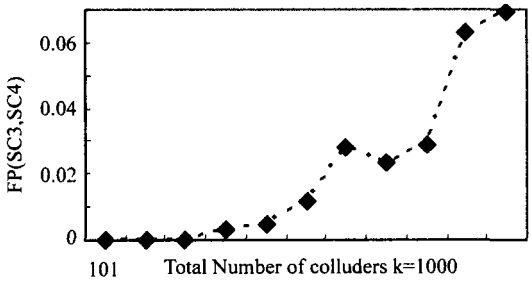

图 4　基于交织共谋攻击的 $FP(SC_{L-1}, SC_L)$分析

Fig. 4　$FP(SC_{L-1}, SC_L)$ per. interleaving based collusion attacks

4　结　论

多播环境下，考虑传输网络的有效带宽以及系统抗击共谋攻击的情况，本文提出了一种基于树结构的高斯分布指纹扩频嵌入技术。与正交扩频指纹系统相比，该系统扩大了用户容量，在共谋攻击者 $K=300$时，该系统俘获其的概率提高了 40%，从而增强了追踪非法用户的能力，进一步提高了指纹加密系统的鲁棒性。

参考文献：

[1] 张峰, 穆晓敏, 杨守义. 数字指纹的研究进展[J]. 电讯技术, 2005, 45(5): 5－10.

[2] WANG Z Jane, WU M, ZHAO H, et al Ray. Resistance of orthogonal Gaussian fingerprints to collusion attacks [A]. IEEE International Conference on Acoustics, speech & Signal Processing[C], 2003, 6－10.

[3] 赵慧民. 一种用于 DRM 的指纹嵌入和解密集成的实现方法研究[J]. 电路与系统学报, 2005, 10(5): 71—75.

[4] COX I, KILLIAN J, LEIGHTON F, et al. Secure spread spectrum watermarking for multimedia[J]. IEEE Trans on Image Processing, 1997, 6(12): 1673－1687.

[5] TRAPPE W, WU M, WANG Z, et al. Anti collusion figerprinting for multimedia[J]. IEEE Tran on Signal Proc, 2003, 51(4): 1069－1087.

[6] WANG Z J, WU M, TRAPPE W, et al. Group-oriented fingerprinting for multimedia forensics[M]. To Appear in EURASIP Journal on Applied Signal Processing, 2004

Research on Method for Spread Spectrum Fingerprints Embedding Following Gaussian Based Tree-Structure

ZHAO Hui-min, ZHANG Hui-le, HU Xue-jun

(Department of Electronic & Information, Foshan University, Foshan Guangdong 528000, China)

Abstract: Digital fingerprint is a new technology to protect multimedia content from illegal copies and redistribution. Under stringent constraints, it is crucial that fingerprinted multimedia copies can resistance collusion attacks in streaming applications. The spread spectrum fingerprints embedding is researched based on tree-structure at multicast following Gaussian with bandwidth requirement. Compared with orthogonal spread spectrum fingerprints embedding technology, the system will be increase of 40% for the probability of capturing colluders depending on the number of users. Therefore, the system improves performance for tracing colluders and further achieves robustness against collusion attacks.

Key words: tree-structure; spread spectrum; Gaussian distribution; fingerprinting system; multimedia video streaming