第7卷第4期　　空军工程大学学报(自然科学版)　　Vol.7 No.4
2006年8月　　JOURNAL OF AIR FORCE ENGINEERING UNIVERSITY(NATURAL SCIENCE EDITION)　　Aug.2006

基于数字指纹的叛逆者追踪技术

韩毅娜[1]，尹忠海[1,2]，简剑锋[2]，王国正[1]
(1. 空军工程大学 电讯工程学院，陕西 西安 710077;2. 西安电子科技大学，陕西 西安 710071)

摘　要:介绍了基于数字指纹技术的叛逆者追踪系统的体系结构及设计原则,给出了非公开密钥、盲检测、变换域、不可见指纹(水印)原则下一种叛逆者追踪系统的工程实现,并进一步讨论了该系统的局限性及尚待进一步研究的技术问题。

关键词:数字指纹;数字水印;叛逆者追踪;DCT变换
中图分类号: TP309　　**文献标识码**:A　　**文章编号**:1009-3516(2006)04-0060-04

近年来,叛逆者追踪技术的研究发展十分迅速,已成为信息安全领域的一个热门课题。与第三方合谋破坏系统安全性的合法授权用户即为叛逆者。基于数字指纹追踪所要考虑的叛逆者主要表现为购买了某数字产品的用户通过网络或其他手段向未授权用户散布、分发该产品的拷贝。本文是在研究和完成了一种非公开密钥、盲检测、变换域、不可见数字指纹的叛逆者追踪系统下,对其技术理论和工程实现的总结。

1　基于数字指纹的叛逆者追踪系统的体系结构

基于数字指纹的叛逆者追踪技术不是防止别人读取数字信息,相反它正是在非法用户成功地读取了这些信息后对其进行追踪。数字指纹的核心技术是指纹信息的嵌入与提取。对于数据中心分发给各最终用户的数字产品(如图片、视频、音频等)在分发以前应在其中分别嵌入代表不同最终用户ID的数字水印信息,这些不同的水印信息即为该用户的指纹。一旦出现泄密或非法拷贝现象,可根据相应的指纹(水印)信息进行泄密追踪,从泄密或非法拷贝数字产品中提取最终用户ID信息,从而实现叛逆者追踪[1]。嵌入与追踪过程如图1、图2所示。

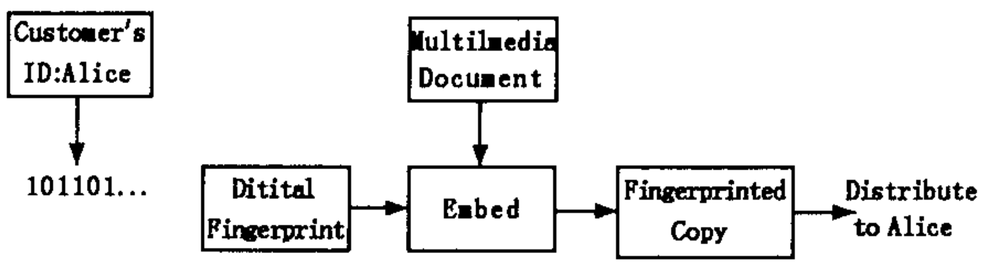

图1　分发给Alice的数字产品嵌入相应的ID图

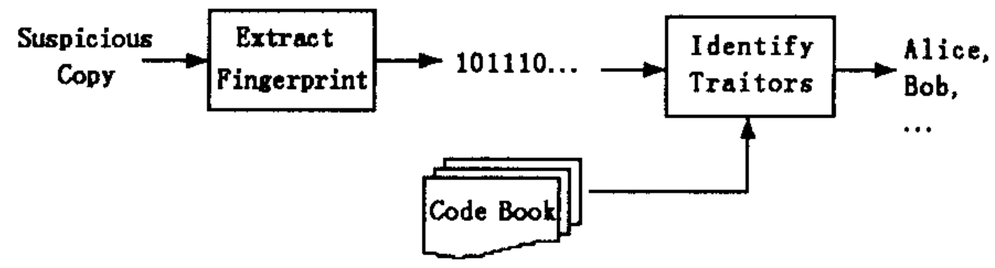

图2　提取疑似泄密数字产品的指纹信息实现叛逆者追踪图

2　数字指纹(水印)的设计原则

根据信息隐藏的目的和技术要求,数字指纹(水印)系统设计应遵循以下原则:

1)实用性(Practicality):实用性主要是指开发的系统应用软件应达到界面友好、操作简便的要求。

2)透明性(Invisibility):指隐蔽载体与原始载体具有充分接近的特性,信息隐藏对人的视觉或听觉系统透明[2],感觉不到隐秘载体的明显变化。

收稿日期:2005-10-14
作者简介:韩毅娜(1965-),女,陕西西安人,硕士生,讲师,主要从事计算机应用技术研究.

3)鲁棒性(Robust):隐秘载体受到一定的干扰(包括滤波、平滑、增强、重采样、有失真压缩、A/D 或 D/A 变换,噪音、几何变换以及人为破坏等),仍然能够恢复秘密信息的能力。

4)密钥及安全性:在本系统中原始图像数量已经非常庞大,随着生产单位、分发单位以及分发时间的不同,一幅图像理论上可对应多个指纹信息及多幅待嵌指纹图像。每一次指纹嵌入均采用不同的密钥(单、双钥),虽然理论上可行,但工程实现存在一定困难。因为不但要保存庞大的密钥库,每次指纹嵌入与提取都要求用户输入不同的密钥,违背了界面友好性及操作方便性原则。基于上述安全上的原因,在本系统的具体实施中计划采用所有图像的指纹产生与嵌入共用唯一单密钥的体制。

5)隐藏的信息量适中:嵌入的秘密信息必须具有足够多的信息以表示多媒体信息的版权或用户 ID 的唯一性,但同时还应满足指纹透明性和鲁棒性。该系统指纹信息按下述原则产生:

生产单位两个字符:× × 如 A6,可编码 36 ×36 =1 296 个不同单位;

分发单位两个字符:× × 如 C8,可编码 36 ×36 =1 296 个不同单位;

分发时间 6 个字符:× × × × × ×,年、月、日分别用两个字符表示。

6)安全性:由于本系统中用密钥确定指纹嵌入的具体位置,即使整个嵌入算法公开,由密钥产生的指纹嵌入与提取位置对攻击者仍是未知的,进一步增强了指纹的抗攻击能力。

7)指纹的唯一性:不同时间分发给不同用户的不同图片的指纹信息应当是唯一的。用户根据该 ID 可判定该图像版权拥有者的详细信息。在本系统的情况下,图像版权拥有者即为泄密者。

综合考虑以上原则,工程中将指纹系统设计成私有的非公开密钥的变换域不可见有意义指纹,指纹的提取采用盲检测技术。指纹嵌入算法借鉴文献[3]中提出的嵌入与提取算法。

3　基于数字指纹的叛逆者追踪系统

系统模型如图 3 所示。本项目主要技术难点集中在高效的抗攻击盲检测的指纹嵌入与提取算法上,算法基本思想是首先将原始图像按 8 ×8 分块,然后伪随机选取一系列 8 ×8 块进行 DCT 变换,利用 JPEG 压缩量化阶段的舍入误差,将经置乱的指纹信号嵌入到部分 DCT 低频系数中,从而完成指纹的嵌入。

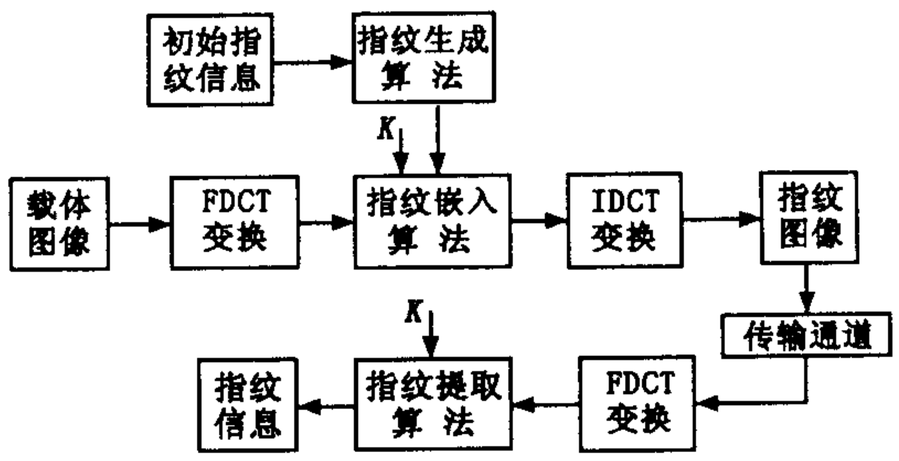

图 3　指纹系统模型

3.1　嵌入指纹的 DCT 块的选择

如图 4 所示,先将原图像 $I(M \times N \times 256)$ 进行 8 ×8 分块,为使指纹信号尽可能地分散,以增强指纹系统安全性,我们用密钥 key 随机选取一系列 8 ×8 的 DCT 块,选择算法同指纹置乱算法。如指纹大小为 8 ×80 =640 且嵌入版本数 $r=1$,则需选择 80 个 DCT 块,如取 $r=3$,则需选择 80 ×3 =240 个 DCT 块。对选定的块可分别进行 8 ×8 离散余弦变换,除以 JPEG 量化矩阵 $\boldsymbol{Q}$ 并进行指纹嵌入。

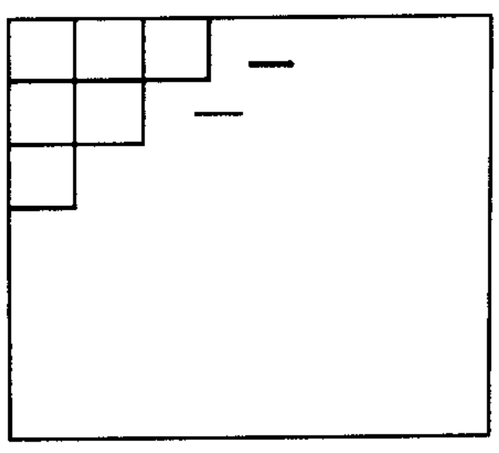
图 4　DCT 块选择图

3.2　嵌入指纹的 DCT 系数选择

不可感知性和鲁棒性是指纹两个相互矛盾的基本要求,有效的指纹算法必须在这两个要求之间进行折中,要保证在不可感知性的前提下,尽可能多地嵌入指纹[1-2]。

经过离散余弦变换,图像的大部分能量集中在低频部分,数值上看低频系数值较大,而高频系数值较小。人眼对于低频区敏感,对于高频区则不十分敏感。将指纹嵌入到图像的高频分量中,能保证视觉透明性。但是,各种图像处理操作对于图像高频部分的损坏可能性大,如有损压缩、低通滤波等。指纹很容易在经历图像处理的过程中损失,稳健性较差;如果要获得很好的稳健性,数字指纹应加在低频部分,但是这样引起的图像降质较大,无法保证视觉透明性。因此为了避开这一矛盾,在本项目中数字指纹的嵌入选在图像的中频部分,用指纹序列对中低频参数进行调制,从而在视觉透明性和稳健性之间进行折中。

具体系数选择方案如图 5 所示,其中标记为 A 的 AC 分量为待嵌入位置,每个选中的 DCT 块共选择其中的 4 个系数用于指纹嵌入。

3.3　指纹嵌入算法

利用量化舍入误差,并结合参照 JPEG 低频系数较高位比特的二值逻辑将指纹嵌入到 DCT 中低频系数中。设当前指纹嵌入次数为 r,按照 DCT 块选择算法先确定一系列 8×8 DCT 系数块,然后将第一个选定块中取定的 4 个 AC 低频分量放入一维矩阵 $\boldsymbol{A}(A=\{A(x),x=0,1,2,3\})$ 中,再对 $\boldsymbol{A}$ 中每一系数进行指纹嵌入,具体嵌入算法如下:

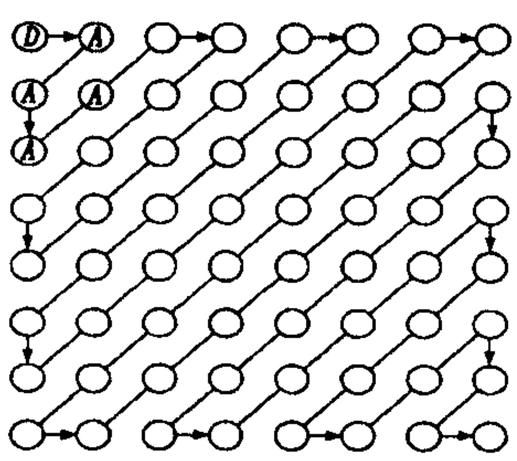

图 5 DCT 嵌入系数选择图

首先取出选定的指纹嵌入位置 DCT 低频系数 A 第 3 位比特,记为 b_3,然后对 A 进行舍入量化以嵌入指纹信号。

用一维数组 Block(i) 表示需嵌入的块,$0\leqslant i\leqslant\dfrac{\lfloor\frac{M}{8}\rfloor\times\lfloor\frac{N}{8}\rfloor}{4}-1$。

// 指纹图像为 $m\times n$, r 为冗余因子。

$$\text{Block}(i)=\begin{cases}1 & 0\leqslant i\leqslant m\times n\times r-1\\ 0 & m\times n\times r\leqslant i\leqslant\lfloor\frac{M}{8}\rfloor\times\lfloor\frac{N}{8}\rfloor/4-1\end{cases}$$

wk = 0; //已嵌入的指纹位数初始化为零,且数组 Block(i)已经置乱。

for i = 0 to $\dfrac{\lfloor\frac{M}{8}\rfloor\times\lfloor\frac{N}{8}\rfloor}{4}-1$

//图像 $I(M\times N\times 256)$,按 8×8 分块每块嵌入 4 位指纹

if Block(i) = 1 then

//第 $\dfrac{i}{\lfloor\frac{N}{8}\rfloor}$ 行第 i mod$\lfloor\frac{N}{8}\rfloor$列 DCT 块应嵌入指纹信息

for j = 0 to 3

if $W(wk+j)\oplus b_3$ $A=2\times\text{round}((A-1)/2)+1$;//量化为奇数,W 为指纹数组。

else $A=2\times\text{round}(A/2)$; //量化为偶数

next j

wk = wk + 4;

end if

next i

之后再把 $\boldsymbol{A}$ 中量化后系数放到原图像中相应的 8×8 块中,直至所有选定的 DCT 块都被嵌入了指纹信号。最后,对每个 8×8 DCT 块先进行 JPEG 反量化后作 DCT 逆变换,然后将各 8×8 块放入载体图像中原来位置,即得到嵌入指纹后的图像 I'。

3.4 指纹提取算法

1) 指纹信号提取:依指纹嵌入步骤确定一系列嵌入指纹的 8×8 块进行 DCT 变换,并进行 JPEG 量化,然后将该块中如图 4 所示的 4 个低频系数放入一维数组 $\boldsymbol{A}$ 中,再按指纹嵌入时同样方法在 $\boldsymbol{A}$ 中伪随机选取一低频系数进行指纹抽取。

2)指纹图像恢复:由步骤 1)获得了含有 r 个指纹版本的指纹信号 W',由于图像经历一些处理操作或攻击后,恢复指纹信号会有一定失真,因此利用这 r 个指纹版本对其进行校正,以减少指纹信号的失真,其基本原理相当于 n/k 表决,具体操作如下:

$$W'_t(t)=\begin{cases}1 & \text{if}\quad\sum_{k=0}^{r-1}W'(k\times m\times n+t)\geqslant r/2\\ 0 & \text{else}\end{cases}\qquad t=1,2,\cdots,m\times n$$

然后利用秘钥 k 对 $\boldsymbol{W'_t}=\{W'_t(t),1\leqslant t\leqslant m\times n,W'(t)\in\{0,1\}\}$ 进行逆置乱变换即为从载体图像中得到的最终指纹信息 $W'_1(t)$。将 $W'_1(t)$ 映射成二维矩阵 $\boldsymbol{W_1}(i,j)$,$\boldsymbol{W_1}=\{W_1(i,j),1\leqslant i\leqslant m,1\leqslant j\leqslant n,W_1(i,j)\in\{0,1\}\}$。这就得到了提取出的指纹图像 $\boldsymbol{W_1}$。

4　系统性能的改进

由于嵌入算法只牵涉到频域中 4 个 AC 系数,对 DCT 变换部分进行简化:设 I 为 8 ×8 块, I'为处理后的 8 ×8 块,I_{ij}为原图像 I 的下标为(i,j)像素, I'_{ij}为处理后 I'的下标为(i,j)像素,63 个 AC 系数记为 $A'_i(i=1,2,\cdots,63)$,处理后 63 个 AC 系数记为 $A_i(i=1,2,\cdots,63)$,在嵌入算法中只有 $A_1 \sim A_4$ 发生了改变,其它系数均未变,即 $A_i = A'_i(i=5,6,\cdots 63)$,设 $A_1 \sim A_4$ 的改变量为 $\Delta A_1 \sim \Delta A_4$,$I$ 处理为 I' 后仅有 $A_1 \sim A_4$的改变 $\Delta A_1 \sim \Delta A_4$ 对 $I'-I$ 有贡献。

$$\mathrm{DCT}(I'-I) = \mathrm{DCT}(I') - \mathrm{DCT}(I) = \{0,\Delta A_1,\Delta A_2,\Delta A_3,\Delta A_4,0,\cdots,0\}$$

其中 $\Delta A_i = A'_i - A_i$,对等式两边取反离散余弦变换后移项得:

$$I' = I + \mathrm{DCT}^{-1}\{0,\Delta A_1,\Delta A_2,\Delta A_3,\Delta A_4,0,\cdots,0\}$$

故在 DCT 变换与逆变换产生 I' 时只须处理 4 个 AC 系数,运算量减为原来的 1/16,经上述调整,系统速度有了大幅提升。

5　研究展望

基于数字指纹(水印)的叛逆者追踪近年来在国际上获得了广泛研究,在基础理论和工程应用方面都获得了相当的进展,但在某些关键技术方面仍待进一步研究和突破。

1)缺少相对统一的关于数字指纹系统的抽象数学模型,限制了理论研究的进一步深入和性能评价标准的建立。

2)数字指纹和数字水印虽然在技术上是相通的,但二者也有明显区别。数字水印技术证明数字产品的版权所有者,即用于版权保护。而数字指纹技术则是主要用于叛逆者追踪。因此基于数字指纹叛逆者追踪必需考虑串谋攻击问题,虽然 Maryland 大学的 MIN Wu 和 K. J. Ray liu 对该问题进行了卓有成校的研究工作,但在算法的计算开销、嵌入的指纹信息量、抗串谋攻击能力等方面距实际工程应用尚有距离,仍有待进一步研究突破。

3)所有叛逆者追踪方案都要求系统具有不可否认性,即要求在技术上仲裁者和数据提供商无法伪造嵌入任何用户指纹的拷贝。在现有的基于数字指纹的叛逆者追踪系统中尚未见到该问题的解决方案。

参考文献:

[1] Boneh D, Shaw J. Collusion – Secure Fingerprinting for Digital Data[A]. In Advances in Gryptology – CRYPTO95, Lecture Notes in Computer Science[C]. York:1995,453 – 465.

[2] 尹忠海. 以改进影像逼真度为约束条件的变换域水印透明性[J]. 西安电子科技大学学报,2005,32(3):339 – 343.

[3] 杨恒伏,陈孝威. 一种鲁棒的 DCT 域公开水印算法[J]. 计算机工程,2003,29(6):142 – 144.

[4] 吴崇明,王晓丹. 数字水印系统的鲁棒性和常见的攻击[J]. 空军工程大学学报(自然科学版),2002,3(1):90 – 93.

(编辑:门向生)

Traitor Tracing Techniques Based on Digital Fingerprinting

HAN Yi – na[1], YIN Zhong – hai[1,2], JIAN Jian – feng[2], WANG Guo – zheng[1]

(1. The Telecommunication Engineering Institute, Air Force Engineering University, Xi'an, Shaanxi 710077, China; 2. Xidian University, Xi'an, Shaanxi 710071, China)

Abstract: In this paper, the architecture and design principles of traitor tracing system based on digital fingerprinting (watermarking) are presented. The realization of traitor tracing system under the condition of private key, blind detection, transform field, invisible fingerprinting is presented, further more, the limitation and the problem to be further studied in the system are also discussed.

Key words: digital fingerprinting; digital watermarking; traitor tracing; DCT transform