多方共享版权的数字水印方案

吴　军[1]，吴秋新[2]

(1. 江西省人民检察院 技术处，江西 南昌 330029；2. 北京机械工业学院 基础部，北京 100085)

摘　要：基于数字水印和密码技术,提出一种由多方共同享有版权的数字媒体版权保护技术。根据可信水印中心存在与否,提出两个多方共享版权的水印方案,经分析,这两个方案均是可行和安全的。

关键词：数字水印；共享版权；秘密共享方案；水印中心；安全信道

中图法分类号：TP309.2　　**文献标识码**：A　　**文章编号**：1001-3695(2005)05-0151-03

Multiparty Shared Copyright Digital Watermarking Schemes

WU Jun[1]，WU Qiu-xin[2]

(1. *Office of Science & Technology, Jiangxi Provincial People's Procuratorate, Nanchang Jiangxi* 330029, *China*; 2. *Dept. of Basic Science, Beijing College of Machine Industry, Beijing* 100085, *China*)

Abstract: Based on watermarking and crytographic techniques, bring forward a digital media copyright protecting technique for the multiparty shared copyright. By a trusting watermarking center existing or not, put forward two mulitiparty shared copyright watermarking schemes. By analysised, they are all feasible and secure.

Key words: Digital Watermarking; Shared Copyright; Secret Shared Scheme; Watermarking Center; Secure Channel

1　引言

数字水印专门研究如何向多媒体数据(如图像、声音、视频信号等)添加某些数字信息,用于标志所有者的版权,并且希望所添加的信息是不可察觉的(某些场合没有这个要求),且不影响数字媒体的正常使用,更重要的是攻击者在不破坏数字媒体本身质量的情况下无法将这些添加的信息去掉。数字水印是目前国际学术界研究的一个热门方向,可为版权保护等问题提供一个潜在的有效解决方案。

目前数字水印研究主要集中在数字水印的嵌入和提取方法上,比如如何选择水印信息的嵌入域,如何将水印信息捆绑到数字媒体中,如何提取或验证水印信息,以及研究所嵌入的水印信息针对有意破坏和普通图像操作的健壮性[3~5]。本文提出一种新的数字媒体版权保护问题,即如果一件数字媒体作品是由多方共同参与创作的,怎么防止其中的某一方或几方瞒着其余方单独宣称拥有版权,侵犯被隐瞒方的利益。目前还没有发现有文献讨论这方面的问题,本文基于数字水印技术,提出两种多方共享版权的水印方案来解决此类问题。

2　数字水印的一般原理

一般的数字水印算法包括两个基本方面:水印的嵌入和水印的提取或检测[1~3]。水印可以是多种模型,如随机数字序列、数字标志、文本以及图像等[4~6]。

设 I 为数字图像,W 为水印信号,K 为密钥或安全参数,则处理后的水印 $\tilde{W}$ 由函数 F 定义为 $\tilde{W}=F(I,W,K)$。水印嵌入过程中,设有编码函数 E、原始图像 I 和水印 $\tilde{W}$,那么嵌入水印后的图像 I_W 可表示为 $I_W=E(I,\tilde{W})$,如图 1 所示。

水印检测是水印算法中最重要的组成部分,其过程如图 2 所示。若将这一过程定义为解码函数 D,则输出的可以是一个判定水印是否存在的 0-1 决策,或带有含义的数据流,如文本、图像等。若已知原始图像 I 和有失真的图像 $\hat{I}_W$,则有:

$$W^*=D(\hat{I}_W,I)\text{ 或 }C(W,W^*,K,\delta)=\begin{cases}1, & W\text{ 存在}\\ 0, & W\text{ 不存在}\end{cases}$$

其中,W^* 为提取的水印,K 为密钥,函数 C 称作相关检测,δ 为决策阈值。检测器的输出结果若充分可信,则可作为版权的潜在法律证据。在实践中,要求水印的检测过程和算法应该完全公开。

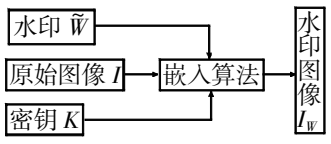

图 1　水印嵌入算法

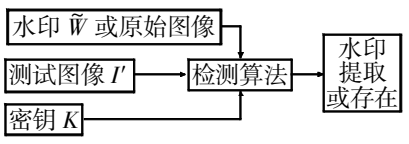

图 2　水印的检测算法

3　多方共享版权的水印方案

3.1　多方共享水印的概念

当一个数字媒体产品是由多方共同创作或生产的时候,如何设计一种水印方案,使得数字媒体产品的版权既能防止外部人员侵权,又能防止内部人员侵权。由于常见的水印方案主要针对外部人员侵权,并没有考虑多方共享版权时的内部人员侵权问题,而内部人员也可能见利忘义地将集体的劳动成果单独拿出去发布,以谋取不正当的利益。另外,可能还会有这样一些情形:①政府介入数字媒体的发布和使用,要求用户必须使用以某些版权为标志的数字媒体;②当知识产权意识变成一种自觉行为时,用户希望自己购买的是正规的有版权的数字媒体

收稿日期：2004-03-18；修返日期：2004-07-24

产品; 等等。这时若数字媒体的版权是由多方共享, 则需要共享版权的各方共同来展示其版权。因此现实生活中确实需要这样的水印方案, 它既能协助解决外部人员的侵权争议, 又能解决多方共享版权时内部人员的侵权争议。本文针对这种情形设计了两种水印方案。

所谓多方共享版权的数字水印方案就是当一个数字媒体作品是多方共同创作或多方共同拥有版权时, 任何一方或少数几方都不能向数字媒体中嵌入或提取数字水印, 只有当所有各方都同时参与时, 才能嵌入或提取水印信息。这种数字水印方案除了上述特点外, 其他特点可与普通数字水印的要求相同。

3.2 存在可信水印中心的多方共享版权的水印方案

假设图像 I 由 $U_1, U_2, \cdots, U_n$ n 个成员共同创作或共同所有, 他们应该共同享有图像 I 的版权, 并且必须防止任何一个成员或一部分成员单独从图像 I 获取利益。普通的水印方案是保护图像免遭外部人员侵犯版权, 而没有考虑版权所有者的其他意图, 所以这种水印方案不能直接满足我们目前所考虑的情形。在这种情形中, 最关键的是每个成员或部分成员不能单独拥有原版图像 I, 也不能单独执行水印的嵌入和水印的提取或检测, 必须是所有的成员一起合作才能恢复原版图像 I 以及产生水印嵌入和水印提取或验证所必需的参数, 然后进一步完成水印的嵌入和提取或验证。当然前提是在图像 I 的创作阶段应能采取措施限制各成员私自拥有图像 I。

下面针对存在可信水印中心时设计一种多方共享版权的水印方案: 假设 T 是一个可信的水印中心, 它向客户提供水印的嵌入和水印的提取或检测服务。服务时对客户的临时秘密信息或密钥进行安全保护, 服务完成后彻底销毁秘密信息或密钥。同时假设 T 可以提供一些额外的基本安全服务。设可信水印中心 T 有一个密码学上的 (n, n) 秘密共享方案和一种安全的对称密钥加密算法, 有一套公开且可靠的带秘密参数或密钥的水印算法。$U_1, U_2, \cdots, U_n$ 共同委托 T 向图像 I 嵌入水印, 必要时共同委托 T 提取或验证水印。

· 第一阶段 水印嵌入过程

(1) 每个成员 U_i 将自己的 ID_i 传送给可信水印中心 T, 并将他们共同拥有的图像 I 和欲嵌入的水印信号模式 w 通过安全信道传送给可信水印中心 T。

(2) 可信水印中心 T 根据所接收到的图像 I、水印信号模式 w、各成员 ID_i, 产生图像 I 的加密密钥 k_I、水印信号 w 的变换密钥 k_w、水印嵌入过程所使用的密钥 k。

(3) 可信水印中心 T 利用一个 (n, n) 秘密共享方案(如一元 n 阶多项式模式), 针对 k_1, k_w, k, 根据成员 $ID_1, ID_2, \cdots, ID_n$, ①计算出: $(ID_1, k_{I1}), (ID_2, k_{I2}), \cdots, (ID_n, k_{In})$, 使这 n 个二元数组恰好可按该 (n, n) 秘密共享方案恢复图像加密密钥 k_I; ②计算出: $(ID_1, k_{w1}), (ID_2, k_{w2}), \cdots, (ID_n, k_{wn})$, 使它们按该 (n, n) 秘密共享方案恢复水印变换密钥 k_w; ③ 计算出: $(ID_1, k_1), (ID_2, k_2), \cdots, (ID_n, k_n)$, 使它们按该 (n, n) 秘密共享方案恢复水印嵌入密钥 k。

(4) 可信水印中心利用 k_w 对水印信号 w 进行变换(具有可逆性)得到 w^*, 根据选定的水印嵌入算法使用密钥 k 将 w^* 嵌入到图像 I 中, 得到加水印后的图像 I^*, 如图 1 所示, 并进行图像 I、水印 w、版权的注册处理。

(5) 可信水印中心利用密钥 k_I 对图像 I 进行加密, 或以 k_I 作为伪随机发生器的种子对图像 I 进行扰乱, 得到图像 $I^{\#}$。

(6) 可信水印中心将七元组 $(ID_i, k_{Ii}, k_{wi}, w, k_i, I^*, I^{\#})$ 通过安全信道传送给成员 U_i, $i = 1, 2, \cdots, n$。

(7) 可信水印中心删除上述处理过程中的一切数据内容, 尤其是涉及到的原始图像和各种密钥, 要彻底毁除。这一步对本协议非常重要。

· 第二阶段 水印提取或验证过程

当 n 个成员需要对某一幅图像 $\hat{I}$ 进行提取水印或验证水印时, 他们必须将各自掌握的数据信息 $(ID_i, k_{Ii}, k_{wi}, k_i)$ 通过安全信道传送给可信水印中心, 可信水印中心利用 (n, n) 秘密共享方案恢复出图像解密密钥 k_I(若水印提取或验证需要原始图像的话)、水印信号逆变换密钥 k_w, 水印提取或验证密钥 k。这里假定水印嵌入过程所使用的各种密钥与水印提取或验证所使用的密钥相同, 然后对按对应的水印提取或验证算法进行水印提取或验证, 并产生结论, 如图 2 所示。可信水印中心将水印检测结论传送给各成员或其他有关人员。

下面针对有可信水印中心的多方共享版权的水印方案进行分析: ①普通的水印方案就是专门针对非版权享有者的侵权, 而我们的水印方案是普通水印方案的扩展, 所以我们的水印方案完全具备防止非版权享有者侵权的功能。②从上面介绍的方案可以看出, 真正用于水印嵌入、水印提取或验证、图像加密或扰乱的密钥是由可信水印中心生成和使用的, 并且水印嵌入、水印提取或验证、图像加密或扰乱、重要数据的删除等各种操作也都是由可信水印中心来完成, 而每个成员只掌握相关密钥共享的影子, 也不能得到原始图像。因此, 共享版权的任何成员都不能单独或少数成员合作恢复出密钥, 因而也就不能进行嵌入水印、提取或验证水印等方面的操作, 所以该方案能够预防数字媒体的版权共享成员的侵权(即内部侵权)。③共享版权的所有成员相互合作并通过可信水印中心能够完成上述各项操作, 而我们在上述方案中已声明: 水印中心是完全可信任的, 而且操作现场数据已及时清除, 不会有重要信息的泄漏, 采用的秘密共享协议是安全的, 因此从密码学的角度来讲, 我们的协议是安全的。综上所述, 在设定的前提下, 该水印方案是可行的。

3.3 无可信水印中心的多方共享版权的水印方案

第 3.2 节描述的多方共享版权的水印方案, 其安全性完全建立在水印中心的可信性的基础之上。如果水印中心一旦不遵守信誉规则, 建立在其上的水印方案将会彻底无效, 所以需要考虑在不存在可信水印中心的情形下, 设计一种数字作品多方共享版权的水印方案。

假设图像 I 是由 $U_1, U_2, \cdots, U_n$ n 个成员共同创作或共同拥有的, 他们对图像 I 共同拥有版权。为保护共同的版权, 他们相互合作设计一个算法可公开的水印嵌入和水印检测或验证的系统。该系统的设计过程如下:

(1) 选择一个通用可靠的水印算法, 在该算法中水印的嵌入和水印的提取或验证都需要使用密钥或者秘密参数。

(2) 设计一个图像和水印信号扰乱器(或称加密与解密器), 其算法具有对称性(即可逆性), 类似于对称密钥算法, 且算法安全性依赖于所使用的密钥。最简单的一种实现方法是

采用伪随机发生器,其种子就是密钥。

(3) 这是最为关键的一步。设计一个安全参数生成部件,它有 n 个输入,分别是 n 个成员各自输入的密钥。输入过程分 n 次进行,每次一个成员输入他的密钥,其他成员回避。它的输出结果是一个安全参数,它可以与 n 个成员输入顺序有关,也可与输入顺序无关。安全参数生成部件可采用单向 Hash 算法来实现。当安全参数生成部件的输出结果用作上述两个系统所需要的密钥时,直接通过可信信道传送给这两个系统,不能让任何人采用任何手段获取这个安全参数,这可以通过分析整个系统是否存在设计漏洞和现场监督来实现。安全参数生成部件与水印系统、图像或水印信号扰乱器相连接时,也要求在连接通道上防止任何比特泄漏。

(4) 设计一个安全的系统运行过程中临时数据的删除算法,以避免运行过程中重要信息泄漏。

利用上述设计的各种系统部件,下面设计一个实现多方共享版权的水印方案,它分两个阶段实施。

第一阶段是水印嵌入过程和图像扰乱处理,其流程图如图 3、图 4 所示。具体步骤如下:

(1) n 个成员共同选择一个水印信号 w,并且每个成员保存一份。成员 U_i 为自己选择三个密钥: k_{wi}, k_i, k_{Ii},并要求长期秘密保存, 这里 $i = 1, 2, \cdots, n$ 。

(2) 按照图 3 的水印算法要求,输入原始图像 I,每个成员各自输入自己的水印变换 H的密钥 k_{wi}和水印嵌入算法密钥 k_i ($i = 1, 2, \cdots, n$) ,输出加水印图像 I_w。

(3) 按照图 4 的图像扰乱算法要求,输入原始图像 I,每个成员各自输入自己的图像扰乱密钥 k_{Ii}($i = 1, 2, \cdots, n$) ,结果输出扰乱图像 ,并将扰乱图像发给每个成员。

(4) 将上述处理过程的系统内部的现场数据进行彻底清除,并删除原始图像 I。

(5) 向水印机构申请版权、水印信号 w、扰乱图像 $I^{\#}$的注册处理。

经过上述过程,每个成员手中只掌握自己的三个密钥 k_{wi}, k_i, k_{Ii}, 水印信号 w和扰乱图像 $I^{\#}$, 其他信息都在水印嵌入完成后现场删除。

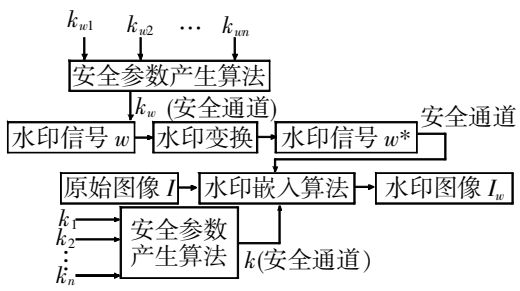

图 3　无可信水印中心的水印嵌入算法

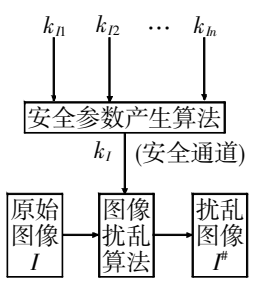

图 4　图像扰乱算法

第二阶段:水印提取或验证过程,系统流程图如图 5 所示。

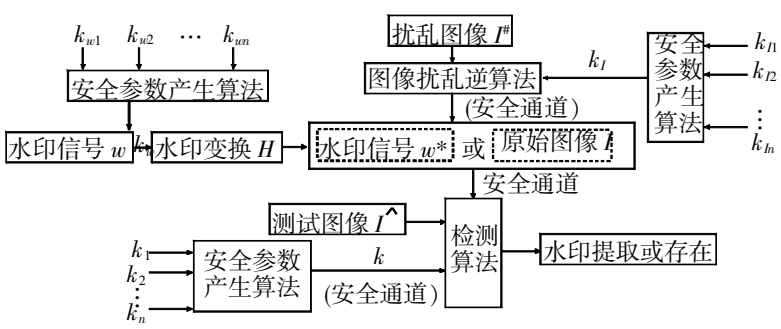

图 5　无可信水印中心的水印检测

当需要提取或验证水印时, n 个成员相互合作, 按照图 4 水印检测系统的要求输入他们各自相应的密钥以及相关的信息,并产生检测结果,以及将水印检测结果传送给有关人员。需要提醒的是,在整个版权保护期间,在水印提取或验证时不能泄漏原图像 I 和 w^* 以及一些检测过程中使用的临时参数,每个成员必须保护好自己的密钥并防止泄漏。

图 4 是考虑水印检测或验证过程中可能需要水印 w^* 或原图像 I 而设计的,在实现过程中,可以根据需要选择相应的部件。

下面讨论无可信水印中心的多方共享版权的水印方案安全性和性能。以上设计的多方共享版权的水印方案,其可行性完全基于水印中心的可信性。当然,在现实世界里这种可信性可能存在也可能不存在,所以我们又针对不存在可信水印中心的情形设计了一种多方共享版权的水印方案。这种水印方案的可行性是基于密码学中类似于多方安全计算基本思想的安全参数生成部件的使用,通过该部件可以使各成员输入自己的密钥后产生一个参数通过安全通道传送给系统其他部件使用,而各成员不会得到该参数的任何信息。

4　结束语

类似于有可信水印中心的多方共享版权的水印方案的分析,无可信水印中心的水印方案能防止共享版权的内部成员单独或少数合谋达到侵犯版权的意图,因为任何共享版权的成员单独或少数合谋都不可能完成水印的提取或验证操作,不能恢复原始图像 I,不能删除加水印后的图像中的水印信号,因而也就像非版权享有者一样不能够有任何侵犯版权的意图而不会被发现。本文提出的方案达到了设计目标,是可行的,也是安全的。

参考文献:

[1] Craver, N Memon, B L Yeo, *et al*. Resolving Rightful Ownerships with Invisible Watermarking Techniques: Limitations, Attacks and Implications [J]. IEEE Journal on Selected Areas in Communications, 1998, 16(4): 573-586.

[2] L T Qiao, K Nahrstedt. Watermarking Schemes and Protocols for Protecting Rightful Ownership and Customer's Rights[J]. Journal of Visual Communication and Image Representation, 1998, 9(3): 194-210.

[3] N Nikolaidis, I Pitas. Copyright Protection of Images Using Robust Digital Signature[C]. Proc. of ICASSP'96, vol. 4, 1996. 2168-2171.

[4] W Zeng, B Liu. A Statistical Watermark Detection Technique Without Using Original Images for Resolving Rightful Ownships of Digital Images[J]. IEEE Trans. Image Processing, 1999, 8(11): 1544-1548.

[5] Wolfgang P, Delp E. A Watermark for Digital Image[C]. Proc. of IEEE Internat Conf. Image Processing'96, Setp 16-19, 1996. 219-222.

[6] I J Cox, Joe Kilian, Tom Leighton, *et al*. Secure Spread Spectrum Watermarking for Multimedia[R]. NEC Technical Report, 1995.

[7] Stefan Katzenbeisser, Fabien A P Petitcolas. 信息伪装与数字水印技术[M]. 吴秋新, 钮心忻, 等. 北京: 人民邮电出版社, 2001.

作者简介:

吴军(1966-),男,江西进贤人,高级工程师,硕士,华中科技大学管理学院博士研究生,主要研究方向为网络信息系统、信息隐藏与数字水印等; 吴秋新(1967-),男,江西吉安人,副教授,博士,主要研究方向为密码算法及密码协议设计、计算机与网络系统安全等。