跨社交网络的隐私图片分享框架

李凤华[1,2,3]，孙哲[1,2]，牛犇[1]，曹进[3]，李晖[3]
（1. 中国科学院信息工程研究所，北京 100093；2. 中国科学院大学网络空间安全学院，北京 100049；
3. 西安电子科技大学网络与信息安全学院，陕西 西安 710071）

摘 要：针对图片转发场景下隐私泄露的问题，提出了一种跨社交网络的隐私图片分享框架，可用于图片隐私信息的延伸控制和溯源取证。延伸控制方案利用基于传播链的访问控制模型限制后续用户的操作权限，并将隐私策略嵌入图片文件，通过图片加密算法保护图片隐私信息和隐私策略的机密性、完整性，确保用户隐私策略被正确执行。该方案不受限于任何现有社交网络图片分享平台，并且能够有效防止非授权转发造成的图片隐私信息泄露威胁。在此基础上，溯源取证方案记录用户的操作行为，并通过嵌套签名方案防止恶意用户篡改和伪造溯源记录，为跨社交网络的图片隐私侵犯行为溯源取证提供技术手段。实验结果验证了所提方案的有效性和效率。

关键词：图片隐私；延伸控制；溯源取证；社交网络
中图分类号：TN 929
文献标识码：A
doi: 10.11959/j.issn.1000−436x.2019107

Privacy-preserving photo sharing framework cross different social network

LI Fenghua[1,2,3], SUN Zhe[1,2], NIU Ben[1], CAO Jin[3], LI Hui[3]
1. Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
2. School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China
3. School of Cyber Engineering, Xidian University, Xi'an 710071, China

Abstract: With rapid developments of digital photography and social networks, users of photo-sharing-supported social networking applications can easily forward photos across different social networks at the cost of their growing privacy concerns. To address this problem, a privacy-preserving photo sharing framework was proposed, which could apply to extended control and privacy invasion tracing. In extended control scheme, the following users on a dissemination chain was restrained by each user's privacy policy. Then several privacy areas of photos were encrypted and the access control polices were bound to the uploaded photos, so that any privacy areas on the photos could be hidden away from unwanted viewers even across different social networks. On this basis, the behaviors of users were record by tracing scheme of privacy invasion, the integrality of records was protected by using nested signature algorithm. The correctness, security and performance of overhead of the scheme are then thoroughly analyzed and evaluated via detailed simulations.

Key words: photo privacy, extended control, privacy invasion tracing, social network

收稿日期：2018−11−06；**修回日期**：2019−04−04
通信作者：牛犇，niuben@iie.ac.cn
基金项目：国家重点研发计划基金资助项目（No.2017YFB0802203）；国家自然科学基金资助项目（No.U1401251, No.61672515, No.61872441）；工业和信息化部 2018 工业互联网创新发展工程项目“工业互联网标识解析数据管理技术标准制定与试验验证”；中国科学院青年创新促进会人才资助项目（No.2018196）
Foundation Items: The National Key Research and Development Program of China (No.2017YFB0802203), The National Natural Science Foundation of China (No.U1401251, No.61672515, No.61872441), 2018 Industrial Internet Innovation and Development Project of China – "Technical Standard Formulation and Verification of Identifier Data Management for Identification and Resolution System", Youth Innovation Promotion Association CAS (No. 2018196)

1 引言

受益于数字拍摄技术和网络技术的持续、快速发展，图片分享社交网络迎来了发展高峰期，社交网络中分享的图片数量不断创造新高。据美国有线电视新闻网报道，Facebook 在 2018 年第二季度报告中提到，其每月活跃用户已达到 22.3 亿个，平均每天上传约 3 亿张图片。在我国，微信朋友圈早在 2015 年的日分享图片数量就已经超过了 10 亿张。社交网络用户通过与朋友分享文字、图片或者短视频来表达情感或分享乐趣。同时，从一个社交网络平台下载信息，并将其转发到另一个社交网络平台，已经逐渐成为社交网络用户的一项日常行为。用户的隐私图片在多信息系统、多边界之间广泛动态流转已成常态。

然而，一旦用户将图片上传到社交网络平台，便失去了对上传图片的控制。任何有权限浏览该图片的用户，都可以不受限制地下载图片，并将其转发到任何地方（线上或线下）。特别是当图片被转发到其他社交网络时，图片所有者几乎不可能再控制图片的传播。近年来，Facebook 泄露门、iCloud 账号泄露等泄露事件频发，使图片隐私信息传播控制成为用户和服务提供商共同关注的问题。另一方面，由于图片中的影像可以直观地反映现实空间中的事物，一些敏感图片的泄露与传播，会影响到公民的生命安全、舆论导向甚至国家利益，严重损害利益相关者的隐私权益，已经引起国家相关部门的高度重视。加强对跨社交网络转发图片的隐私侵犯行为监管，并对已发生的隐私泄露事件进行溯源取证也愈发重要。

为解决上述问题，近年来研究者在图片隐私信息传播控制和溯源取证方面都提出了大量的解决方案。在隐私图片传播控制方面，现有方案大多采用基于访问控制技术[1-6]或者加密技术[7-10]等机制。其中，基于访问控制的方案[1,3,6]通常假设应用系统可以控制上传到指定平台的图片，但是该假设难以应用到跨社交网络的转发场景中。现有的基于加密的图片隐私保护方案[7-8]较少考虑访问控制策略，访问者能否访问加密的隐私区域完全依赖访问者是否拥有密钥。目前，研究者们将针对转发后数据的访问控制技术称为延伸控制[11]。Karjoth 等[12]提出了隐私保护方案 Sticky Policy，将访问控制策略嵌入绑定到文件上，实现了跨系统的隐私保护，并迅速成为云计算领域中一种热门的跨云信息保护解决方案。然而，由于图片本身的复杂性和展示问题，该类方法并不能直接运用于图片分享社交网络中。另一方面，溯源取证方案[13-14]大多将隐私信息与溯源记录分开存储，例如基于起源信息的溯源系统[15]，当隐私信息离开信息系统后，便失去了隐私信息保护策略标准，无法对隐私信息是否违背所有者意愿进行判断。而基于边界管控[16]和事后审计[17]的溯源方案，难以汇集分散在各个信息系统中的溯源信息，缺乏统一的溯源信息分析和取证能力。

本文为隐私敏感的用户提出了一种跨社交网络的隐私图片分享框架，从图片传播的角度出发，分别应用于延伸控制（正向）和溯源取证（逆向）2 个场景中。具体地，该方案将隐私标记和访问控制策略绑定到图片中，并利用加密方法保证图片的隐私区域在传播到其他社交网络时，仍只有拥有权限的用户才能访问。同时，通过在隐私标记中增加溯源记录信息的方法，使隐私泄露事件发生后，取证人员可以对隐私侵犯行为进行溯源取证。本文主要贡献如下。

1) 提出了一种跨社交网络的隐私图片分享框架，使图片在被转发后其所有者仍可以限制转发用户的转发行为，并在隐私泄露后可以对隐私侵犯行为进行溯源。该框架针对图片文件的特点，选用支持区域加密的算法，并设计一种基于图片元数据的策略嵌入方法，避免绑定的策略影响图片公开区域的正常显示。

2) 设计了一种基于信息传播链的访问控制模型，该模型允许传播链上的用户按先后顺序为图片设置策略，限制后续用户的操作权限和可赋予权限。

3) 提出了一种双层加密算法来保护图片的隐私区域和访问控制策略。双层加密方案分别用于保护访问控制策略和图片中的隐私区域。

4) 提出了一种嵌套签名算法，在追加溯源记录信息时将先前用户的溯源记录与新溯源记录进行嵌套签名，保证隐私标记中的用户操作行为记录不被恶意用户篡改和伪造。

2 相关工作

随着社交网络中传播图片数量的不断增长，图片分享中的隐私泄露问题已经引起了研究者们的广泛关注[18-21]。本文涉及图片隐私保护、溯源取证

等多个研究热点。

2.1　图片隐私保护方法

为帮助用户控制隐私图片的分享范围，现有的隐私图片保护方法主要包括基于访问控制方法、基于密码学方法和复合方法。

1) 基于访问控制的方法

在早期的工作中, Hu 等[1]提出了一种多主体访问控制机制，尝试通过量化隐私风险和分享收益损失来解决不同角色的隐私冲突。该方法通过引入一个投票机制，让包括转发者在内的所有角色都可以参与到访问控制策略的决策中。随后，Illy 等[2]提出将访问控制粒度从图片级转换为人脸区域级，从客体粒度上规避了不同主体的隐私冲突，然而，该方法仅对人脸区域有效。在此基础上，Vishwamitra 等[3]通过引入其他细粒度客体，将隐私区域从人脸扩展到物品、背景、人体等区域，当多主体对同一个隐私区域存在隐私冲突时，仍将使用一个投票机制来确定该区域的隐私策略。为了提高图片的访问控制效率, Xu 等[4]提出了一种基于分布一致性的访问控制方法，该方法识别出上传图片中的用户，并通知用户就隐私策略与图片发布者协商一致。然而，上述方法实现访问控制需要保证图片所在环境的可控，因此很难处理隐私图片跨社交网络转发的情况。此外，该类方法将转发者与图片共享中的其他角色一样对待，忽略了转发用户与前一个用户的隶属关系。

2) 基于密码学的方法

为保障图片在离开原系统后不被泄露，现有基于加密的图片隐私保护算法主要集中在存储阶段，将焦点聚集在避免加密图片被暴力破解和提高系统的运行效率上[8,10,22-23]。Ferreira 等[24]提出了一种安全存储和检索的框架，允许用户在密文状态下查询上下文。Ra 等[7]提出了一种支持区域加密的方案，该方案将整张图片划分为公开和隐私两部分，可以实现只加密图片的隐私部分而不影响图片公开部分的展示。在此基础上，Yuan 等[25]扩展了 Ra 的方案[7]，设计了一种支持多个隐私区域的加密方案，通过给不同的隐私区域设置不同的密钥，实现向不同用户展示不同隐私区域的目的。为了提高图片的加密效率，Nourian 等[26]提出了一种基于混淆映射的加密算法，该算法通过混淆图片数据的编码方案实现对图片可视区域的信息隐藏，支持图片在混淆状态下的像素级操作，并实现了多种像素级的过滤算法。尽管文献[7, 24-26]的解决方案可以较容易地应用在社交网络上，但是它们都存在将访问策略与管理密钥相互映射的难题。

3) 复合方法

在早期的工作中, Karjoth 等[12]提出了一种粘性政策的复合方法，将访问控制策略绑定到原始数据上，从而解决跨系统传播的问题。此后，该类方案在跨云隐私保护中流行起来。Pearson 等[27]提出了一种实用的跨云隐私保护框架，通过将隐私数据与安全策略绑定，实现隐私数据的跨云控制。Spyra 等[28]设计了一种基于身份的加密方案（IBE，identification-based encryption），该方案在考虑云后台保密性、完整性和可靠性的基础上，提高了绑定策略的安全性。尽管前面提到的工作可以有效解决跨云服务场景中的隐私保护问题，但由于图片文件的特性，该方案不能直接用于图片分享社交网络。

2.2　隐私侵犯行为溯源取证方法

在隐私信息跨信息系统传播的过程中，溯源信息需要在不同信息系统间广泛交换。现有的溯源取证方案[13-14]大多聚焦于单一信息系统内部，当隐私信息流转出信息系统边界后，便失去控制和溯源取证能力，并没有针对多应用系统、多边界的隐私信息广泛动态流转场景中溯源取证问题提出解决方案。另一方面，现有信息系统中隐私信息与保护策略大多分开存储，例如基于起源信息的方案[15, 29-30]，将信息的演化脉络存储在起源信息中，当隐私信息离开信息系统后，便失去了隐私信息保护策略标准，无法对隐私信息是否违背隐私信息所有者意愿进行判断。

在隐私信息跨系统、跨边界流转过程中，所采集、记录、存储的溯源取证信息存在不可伪造和不可篡改的需求。现有信息系统间的隐私溯源方法主要依靠边界管控技术[16]和事后审计技术[17]，当隐私信息离开或进入信息系统时，对隐私信息的传播途径进行记录，供泄露事件发生后进行安全审计和取证分析。该类方案的缺陷在于不同的信息系统边界上缺乏统一的溯源信息汇聚和分析能力，难以实现对不同信息系统边界的采集汇总和溯源取证。

3　预备知识

3.1　跨社交网络转发场景用户调研

在日常生活中，为避免图片未经允许地转发给

其他用户，甚至转发到其他社交网络中，一些隐私敏感的用户会选择不上传任何图片以保护自己的隐私，然而这样就失去了一种表达情感的方式，明显地违背了社交网络建立的初衷。为调查目前用户对支持图片分享社交应用的使用情况，本文展开了一项调研，分别从中国用户和美国用户中收集了 339 份和 148 份调查问卷。如表 1 所示，总体上 41.27%的参与者在手机上安装了 1~5 个支持图片分享的应用，在美国 58.78%的用户在手机上安装了 10 个以上的图片分享应用。综上所述，绝大多数用户在手机上安装了超过一个图片分享应用。

表 1 用户手机上安装的图片分享应用数量

安装应用个数	中国		美国		总体	
	用户数/个	占比	用户数/个	占比	用户数/个	占比
未安装	13	3.83%	2	1.35%	15	3.08%
1~5 个	**172**	**50.74%**	29	19.59%	**201**	**41.27%**
6~10 个	76	22.42%	30	20.27%	106	21.77%
10 个以上	78	23.01%	**87**	**58.78%**	165	33.88%

而另一方面，目前，Facebook、微信等图片分享服务商只能提供较少的隐私保护机制，尤其是市面上几乎没有跨社交网络转发的延伸控制机制。在学术界，虽然 Pearson 等[27]尝试通过将访问控制策略绑定到文件上来解决跨系统传播的问题，但是由于该方案并非针对图片文件，无法适应图片文件的一些特殊属性，很难直接应用到支持图片分享的社交网络中。此外，隐私图片文件往往比一般文件更加复杂，通常会包括多个隐私区域和公开区域。因此，针对图片分享社交网络的实用延伸控制机制仍值得深入研究。

本文的主要研究思路是通过探索一个实用的框架来保护用户图片分享过程中的隐私信息，尤其是图片被转发到其他社交网络后，依然可以遵从图片所有者、先前图片转发者的意愿进行传播和处理。具体来说，本文提出的隐私图片分享框架应当解决以下几个问题。

1) 针对现有访问控制模型未将转发者作为一种特殊角色处理的问题，设计了一种基于传播链的访问控制模型，解决用户对转发后隐私图片的权限分配问题。

2) 针对图像加密算法跨社交网络传播时密钥管理困难的问题，提出了一种双层图片加密算法，第一层使用对称加密保护图片上的隐私区域，第二层使用公钥加密算法保护用户的访问控制策略，根据策略赋予解密的权利。

3) 针对图片文件特征复杂的问题，设计了一种支持图片特征的策略嵌入方法，且绑定的策略不会影响图片公开区域在社交网络传播中的正常显示。

4) 针对图片隐私溯源记录跨社交网络流转时抗篡改和抗伪造的需求，提出了一种嵌套签名方案，通过将先前用户签名的记录与自己的记录一同签名，防止恶意用户在图片流转过程中篡改溯源记录信息、伪造证据。

3.2 攻击模型和隐私保护目标

1) 攻击模型

为实现跨社交网络的隐私图片分享，本框架将攻击者的攻击归纳成以下 3 种方式：①攻击者 attacker1 试图通过留存、篡改、伪造访问控制策略的方式，获取没有访问权限的隐私信息；②攻击者 attacker2 是系统内部的用户，拥有部分权限，并试图利用已有权限获得更多的权限；③攻击者 attacker3 知晓策略嵌入或者溯源记录格式等背景知识，试图通过篡改、伪造访问控制策略或溯源记录，掩盖隐私侵犯行为痕迹。

为保障隐私图片在跨社交网络流转过程中的安全性和完整性，本框架基于现有的密码学技术，如图像区域加密、公钥密码基础（PKI, public key infrastructure）等体系，通过对各个实体间所传输的图片隐私区域和访问控制策略进行加密操作，以保证隐私图片在传输过程中的安全，避免窃听、截取等被动攻击的发生。因此本方案仅对常见的几种加密方法进行安全性对比，不再对上述安全问题进行详细的安全性证明。

2) 隐私保护目标

基于以上攻击模型，当隐私图片在不同社交网络流转时，系统内外用户均不能获取未授权的隐私信息；系统内用户除了被分配的权限以外，无法绕过权限分配者获取更多的操作权限；隐私侵犯行为可以溯源追踪，攻击者无法通过篡改、伪造溯源记录遮掩隐私侵犯行为。

4 隐私图片延伸控制与溯源取证

4.1 隐私图片延伸控制

本节首先介绍跨社交网络隐私图片延伸控制的应用场景、系统框架，然后对所提方案内容和实现细节进行详细介绍。

4.1.1　系统模型

图 1 描述了跨社交网络图片分享的系统模型，在该模型中所有的用户被分为以下 3 种角色。

1) 图片所有者（photo owner）：第一个发布图片的用户。

2) 图片转发者（photo forwarder）：接收到图片并将其转发的用户。

3) 静默的接收者（silent receiver）：接收到图片并无传播操作的用户。

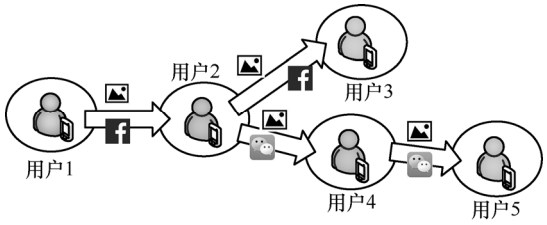


图 1　跨社交网络图片分享的系统模型

在图 1 的模型中，用户 1 是图片所有者，用户 2 和用户 4 是图片转发者，用户 3 和用户 5 是静默的接收者。用户 1 将图片上传到 Facebook 中，用户 2 接收到图片后转发给 Facebook 中的用户 3，同时将图片从 Facebook 下载并转发到微信中的用户 4。用户 4 在微信中将其转发给用户 5。整个流程跨越了 Facebook 和微信 2 个社交网络，且在 2 个社交网络内部都存在转发行为。本文将 3 种角色结合，共同组成一个链状结构，称之为传播链。传播链描述了一条图片传播的路径，例如：用户 1—用户 2—用户 3 是一条 Facebook 内部的传播链，用户 1—用户 2—用户 4—用户 5 是一条跨 Facebook 和微信 2 种社交网络的传播链。

本文为跨社交网络图片转发中的隐私保护问题设计了一种解决方案，该方案也可应用在单一社交网络内部。居于传播链上的用户都可以对后续用户的访问权限和延伸控制权限进行控制。本方案主要包括层次化部署架构、基于传播链的访问控制模型和双层加密算法，并在实现细节中详细介绍了访问控制策略的嵌入方法。

4.1.2　系统框架

延伸控制系统框架主要包括以下 2 个部分：1）一个用于保护图片隐私区域和匹配访问控制策略的客户端；2）一个用于管理密钥的服务器。在系统中，所有的本地客户端组件（包括操作系统、应用程序、传感器等）和密钥管理中心被认为是可信的，传播信道和社交网络服务提供商被认为是不可信的。

在系统中，客户端在发送时可以对图片中的隐私区域进行第一层加密，这些隐私区域可以通过相同或者不同的密钥进行加密。用户可以对隐私区域设置访问控制策略和延伸控制策略并进行第二层加密，再通过客户端将策略绑定到图片中。当图片被上传到一个公开的社交网络时，社交网络扮演了用户间沟通桥梁的角色。

用户收到图片后，可以请求查看或者转发图片。客户端通过向服务器请求，验证用户身份，并对图片上绑定策略进行“解锁”。只有符合访问控制策略规定权限的用户才能访问图片的隐私区域。接收用户在转发图片时可以追加新的策略，在转发图片时设置的策略必须是延伸控制策略的子集。因此，通过设置延伸控制策略，传播链上的用户可以限制后续用户的传播行为。

如图 2 所示，用户 1 加密了图片上 2 个隐私区域，并生成相应的访问控制和延伸控制策略。当图片被发布到公开的社交网络时，用户 1 的策略随图片一起上传。用户 2 下载图片，并根据图片上绑定的策略判断是否能浏览图片上的隐私区域。与此同时，用户 2 还可以根据用户 1 赋予的延伸控制权限增加新的权限，并可以继续设置用户 3 可以浏览隐私区域 1，用户 4 可以浏览隐私区域 2。用户 4 可以继续追加策略，禁止用户 5 浏览所有的隐私区域。

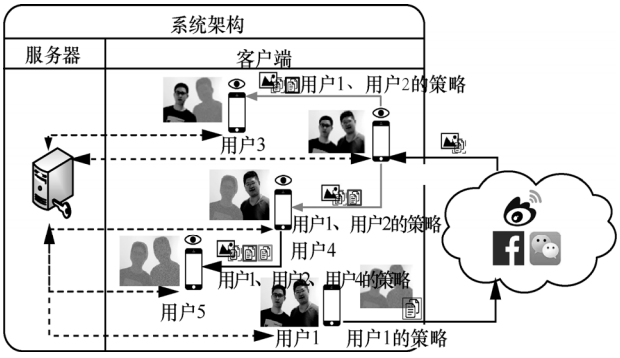


图 2　延伸控制系统架构示例

4.1.3　基于传播链的访问控制

在本方案中，权限根据传播链依次授权，其中传播链是由社交网络中的多次图片交换组成。定义图片 p 的第 i 次交换为 $E_i=(s_i \to r_i, p)$，其中 s_i 和 r_i 分别是第 i 次交换中的发送者和接收者。因此传播链可以被定义为一个有序集合

$$D=\langle E_1,E_2,\cdots,E_n\rangle \tag{1}$$

根据传播链有序集合 D 的连续性，下一次图片交互的发送者为前一次图片交换的接收者，即 $s_{i+1}=r_i$。第一个发送者 s_1 是图片所有者，最后一个接收者 r_n 是静默接收者，其他所有用户都是图片转发者。

基于传播链的约束条件用于明确发送者可以分配给接收者何种权限的约束，可以用一个通用格式来描述这个约束，如式(2)所示。

$$\begin{aligned}&\mathrm{PrA}_i=\left(E_i,\mathrm{PrA}_{i,1},[\mathrm{PrA}_{i,2}]\right)=\\&\qquad\left(\left(s_i\to r_i,p\right),\left(c_1,\mathrm{pr}_1\right),\left[\left(c_2,\mathrm{pr}_2\right)\right]\right)\end{aligned} \tag{2}$$

其中，$E_i=\left(s_i\to r_i,p\right)$ 表示权限是第 i 次交换 E_i 中发送者 s_i 分配给接收者 r_i 的，访问控制客体为图片 p；$\mathrm{PrA}_{i,1}$ 定义了接收者 r_i 的权限，而 $\mathrm{PrA}_{i,2}$ 定义了接收者 r_i 可以分配其下一个用户什么权限；方括号表示参数 $\mathrm{PrA}_{i,2}$ 是可选的，当参数 $[\mathrm{PrA}_{i,2}]$ 选择为空时，则表示 $\mathrm{PrA}_{i,2}=\mathrm{PrA}_{i,1}$。此外，为保证延伸控制，传播链上后面的用户不能被分配高于先前用户的权限，即 $\mathrm{PrA}_{i,2}\subseteq\mathrm{PrA}_{i,1}$。在等式 $\mathrm{PrA}_{i,x}=\left(c_x,\mathrm{pr}_x\right)$，$x=1,2$ 中，c_x 表示一个约束条件集合，如时间、位置、用户关系等；pr_x 表示一个权限集合，比如查阅、转发等。

以图 2 为例，用户 2 允许用户 4 浏览图片中的隐私区域 2，但是禁止用户 4 分配用户 5 浏览图片中隐私区域 2 的权限，则该策略可以表示为 $((\mathrm{user}_2\to\mathrm{user}_4,\mathrm{area}_2),(\mathrm{user}_4,\mathrm{view}),(\mathrm{user}_5,\mathrm{prohibit\ view}))$，其中，user 表示用户，$\mathrm{area}_2$ 表示隐私区域 2，view 表示浏览权限，prohibit view 表示禁止浏览。

4.1.4 双层加密算法

为满足用户的隐私需求，当图片上传到社交网络后，加密算法需要确保图片上的隐私信息不对无权限用户展示，从而保证传播链上先前用户的策略会被严格执行。本文假设框架中每个用户至少拥有一个客户端，并且密钥管理中心给每个用户分配一个公私钥对。

为保证图片在社交网络传播中的正常显示，需要保证：图像加密算法在加密隐私区域的同时不会影响公开区域的图像显示；附加的策略不能破坏图片的固有格式，应当嵌入到标准图片格式的自定义区域。

1) 第一层图像加密

本文方案中，采用文献[25]中的扰动算法对图片隐私区域进行加密。该算法通过修改 JPEG（joint photographic experts group）文件的离散余弦变换（DCT, discrete cosine transform）系数来达到加密效果。

隐私区域选定与参数设置：该算法将图片划分成16像素×16 像素的最小编码单元，生成一个遮掩矩阵 $\boldsymbol{M}$，$\boldsymbol{M}$ 中的非零元素代表用户选定的隐私区域序号。因此，所有用户标记的隐私区域都是由一个个小方格（最小编码单元）组成的，并且每个隐私区域不会重叠，即每个最小编码单元只能拥有一个区域序号，序号 0 代表公开区域。针对每个隐私区域 region_n，用户都可以分配一个密钥 key_n 和一个加密强度等级 $\mathrm{level}_n\in\{\mathrm{low},\mathrm{medium},\mathrm{high}\}$。

加密流程：将 DCT 系数量化为一个 8×8 的 DCT 矩阵，记为 $\boldsymbol{x}_i\left(i=1,2,\cdots,64\right)$，通过密钥 key_n 作为种子生成一个随机序列 $\mathrm{random}_i\in\{1,-1\}$，通过将 DCT 系数矩阵 $\boldsymbol{x}_i$ 与随机序列 random_i 实现对图片像素的加密。针对不同加密强度的需求，根据加密强度等级 level_n 进行不同程度的扰动处理。当 $\mathrm{level}_n=\mathrm{low}$ 时，系统仅修改图像 YUV 这 3 个色彩分量（其中，Y 表示亮度，即灰度值；U 和 V 表示色度，用于描述影像色彩及饱和度）中的 AC（alternating current）系数；当 $\mathrm{level}_n=\mathrm{medium}$ 时；修改亮度分量的 AC 系数和 DC（direct current）系数；当 $\mathrm{level}_n=\mathrm{high}$ 时，修改 3 个色彩分量（YUV）的 AC 系数和 DC 系数。

2) 策略嵌入与第二层加密

为保障绑定的策略不会影响图片公开区域在社交网络中的正常显示，本文设计了一种新的访问控制嵌入方法，通过将策略嵌入图片的 EXIF（exchangeable image file）元数据中的 IFD（image file directory）结构中，避免修改现行的文件格式，从而很好地兼容现有的图片分享平台。EXIF 元数据被广泛用于各种图片文件格式，如 JPEG、RAW、TIFF（tag image file format）、RIFF（resource interchange file format）等。

嵌入策略的格式包含固定和可变 2 个部分。固定部分包含图片隐私区域坐标、拍摄时间、拍摄地点等固定属性，可变部分可以存放数量动态变化的访问控制策略。如图 3 所示，由于 IFD 结构本身是一种嵌套结构，包括本级 IFD 的数据域和多条子 IFD 结构。本方法将访问控制策略（以及第 4.2 节中的溯源记录）的语法作为一条子 IFD 结构，每增加一条策略（或记录）时，动态增加

一条子 IFD 结构。当一个图片被转发时，嵌入的策略将随着图片一起在不同的社交网络中流转。嵌入策略分配的权限应当遵从基于传播链的访问控制模型的约束。

在使用对称密钥实现第一层图片隐私区域加密的基础上，本方案利用公钥密码基础（PKI, public key infrastructure）方案来保护策略的机密性和完整性。在信息传播链上的用户需要通过公钥将嵌入在图片上的访问控制策略“解锁”，从而保证策略在图片流转过程中没有被其他用户篡改。

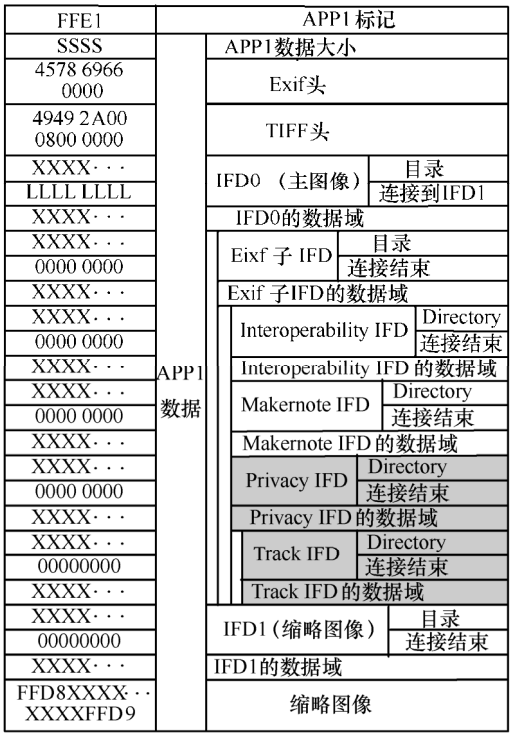


图 3　EXIF 嵌入策略

3) 性能优化

传统 C/S（client/server）架构在整个分享系统中用户数量较少时还可以正常运行。然而，随着社交网络中传播图片数量的飞速增长，即使用户给每张图片上的所有隐私区域都分配一个密钥，服务器端也将面临海量图片加解密和密钥管理的挑战。

本节基于边缘计算原理设计了一种层次化的部署架构，如图 4 所示，该架构包括 3 个部分：核心服务器、边缘服务器、终端设备。

核心服务器：负责验证所有用户的身份，并负责给系统所有用户分配公私钥对。

边缘服务器：负责管理部分用户发布和转发图片的密钥，并为一些计算能力不足的移动设备提供图片加解密服务。

终端设备：作为与用户交互的终端，并同时承担一定程度的计算任务，包括对图片访问控制策略和延伸控制策略加解密、溯源记录信息签名验签、部分计算量较小的图片加解密任务。

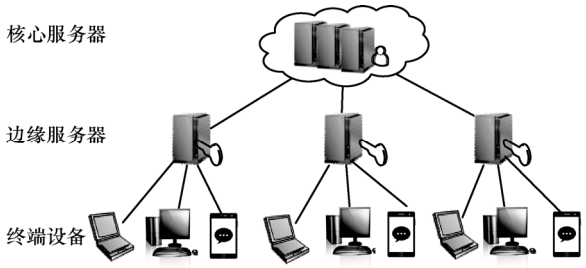


图 4　基于边缘计算原理的层次化部署架构

在整个架构中，用户（拥有同一账户的移动终端）被分配到不同的边缘服务器中，其对应发布图片的加解密密钥被保存在这些边缘服务器中，并备份到核心服务器。当有新图片被转发到边缘服务器管理的用户中时，边缘服务器可以向核心服务器申请该图片的加解密密钥。受限于边缘服务器的资源，可以引入缓存机制来解决边缘服务器的存储容量问题。此外，由于所有的访问控制和延伸控制策略都嵌入在图片中，架构中的设备并不需要存储和更新图片的策略。整个系统仅需要对策略和隐私区域的密钥进行同步。

图片隐私侵犯行为溯源取证作为隐私图片延伸控制的逆向过程，也面临跨社交网络溯源的难题。相较于图片隐私信息的正向传播，溯源取证方案对溯源记录信息防篡改和防伪造提出了更高的要求。然而，目前跨社交网络图片隐私侵犯行为溯源取证的相关研究还比较少，本文在图片隐私延伸控制的基础上，设计了一种适用于跨社交网络场景的图片隐私侵犯行为溯源取证方案。

4.2　图片隐私侵犯行为溯源取证

图片隐私侵犯行为溯源取证的任务主要指通过对流转中的图片隐私信息进行统一描述，当图片开始流转时，不断记录不同社交网络中不同主体对图片隐私信息执行的操作，通过对比隐私侵犯行为判定标准，判断是否发生隐私侵犯行为。

4.2.1　图片隐私侵犯行为溯源取证场景

图 5 描述了图片在用户分享过程中的传播途径，整个传播路径呈树状结构，根节点是图片所有

者, 叶节点是静默接收者, 中间节点为图片转发者。假如传播过程中, 隐私图片多次经过同一个用户 2, 则将用户看作多个节点, 即用户 2 第一次转发节点（节点 2）、用户 2 第二次转发节点（节点 6）。其中, 树结构的深度表示图片隐私信息的转发次数。因此, 从任何节点出发向根节点溯源, 都可以获得一条唯一的无环溯源链（反向）, 例如图 5 中, 节点 11—节点 5—节点 2—节点 1 即是一条无环溯源链。

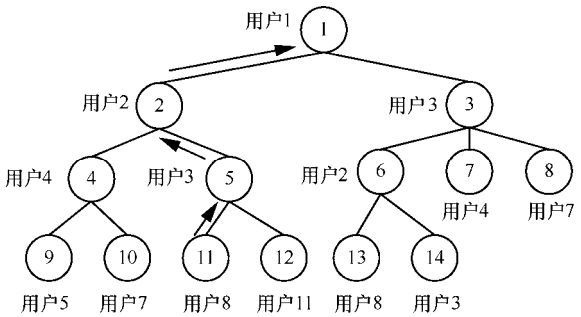


图 5 传播路径

图片隐私侵犯行为溯源取证方案包括以下 2 个阶段。

1) 溯源信息记录阶段。在图片开始流转时, 由图片所有者创建溯源标识, 包括隐私信息、隐私信息判定标准、溯源记录信息。在图片传播过程中, 每流转到一个用户时, 通过插件将用户对图片隐私信息执行的分享操作、处理操作和行为发生环境记录在溯源信息记录中, 并利用嵌套签名保障图片在传播过程中不被恶意篡改和伪造。该阶段可以合并到延伸控制机制完成。

2) 溯源取证阶段。当图片隐私泄露情况发生时, 从发现情况的节点出发, 向根节点方向溯源, 即可获得一条图片隐私信息的溯源链。取证人员通过验签确认溯源标识的完整性, 并根据溯源记录信息和隐私侵犯行为标准判定是否有隐私行为发生。

4.2.2 嵌套签名算法

为了保证图片隐私信息在传播过程中不被恶意用户篡改和伪造, 本文溯源方案设计了一种嵌套签名算法。通过使用该算法, 图片所有者创建溯源标识, 生成第一条溯源记录信息并签名；后续每一个图片转发者对先前记录验签后, 将自己的操作行为记录与先前溯源记录信息及其签名合并进行签名；当进行隐私侵犯行为判定时, 取证人员需对溯源记录进行逐层验签, 来确认各个节点的溯源记录是否被恶意篡改和伪造。整个过程由延伸控制系统算法插件自动执行, 嵌套签名形式化描述如下。

1) 图片所有者 owner 创建溯源标识 TraTag。

$$\mathrm{TraTag}=\langle \mathrm{Pri},\mathrm{Pol},\mathrm{Rec}\rangle \tag{3}$$

其中, Pri 为隐私信息, Pol 为隐私侵犯行为判定标准, Rec 为溯源记录。隐私侵犯行为判定标准 Pol 可与延伸控制的访问控制策略保持一致。

溯源记录函数定义为

$$\mathrm{REC}: S\times O\times 2^{\mathrm{OP}}\times 2^{\mathrm{CON}}\times \mathrm{Sig}_{\mathrm{user}}\rightarrow \mathrm{Rec} \tag{4}$$

其中, S 表示操作主体、O 表示操作客体（记录隐私信息当前散列值）、$\mathrm{OP}=\{\mathrm{op}_1,\mathrm{op}_2,\cdots\}$ 表示操作行为集合、$\mathrm{CON}=\{\mathrm{con}_1,\mathrm{con}_2,\cdots\}$ 表示操作行为发生的环境集合、$\mathrm{Sig}_{\mathrm{user}}$ 表示用户 user 签名值。

签名函数定义为

$$\mathrm{SIG}:\mathrm{Rec}\times S\times O\times 2^{\mathrm{OP}}\times 2^{\mathrm{CON}}\rightarrow \mathrm{Sig}_{\mathrm{user}} \tag{5}$$

则图片所有者 owner 创建的溯源记录为

$$\mathrm{Sig}_{\mathrm{owner}}=\mathrm{SIG}(S_{\mathrm{owner}},O_{\mathrm{owner}},\mathrm{OP}_{\mathrm{owner}},\mathrm{CON}_{\mathrm{owner}}) \tag{6}$$

$$\mathrm{Rec}_{\mathrm{owner}}=\mathrm{REC}(S_{\mathrm{owner}},O_{\mathrm{owner}},\mathrm{OP}_{\mathrm{owner}},\mathrm{CON}_{\mathrm{owner}},\mathrm{Sig}_{\mathrm{owner}}) \tag{7}$$

2) 根据接收的溯源记录 $\mathrm{Rec}_{\mathrm{owner}}$, 图片转发者 $\mathrm{forwarder}_1$ 的处理流程如下。

Step1 验证接收溯源记录信息的签名值 $\mathrm{Sig}_{\mathrm{owner}}$。如果验签通过, 则进入 Step2；如果签名值不匹配, 则认为溯源记录被恶意篡改, 跳转至 Step 4。

Step2 比较溯源记录中操作客体 O_{owner} 的散列值 $\mathrm{Hash}_{\mathrm{track}}$ 与自身接收到的图片隐私信息散列值 $\mathrm{Hash}_{\mathrm{receive}}$ 是否一致。如果一致, 则进入 Step3；否则认为图片隐私信息与溯源记录不匹配, 溯源记录被恶意篡改, 跳转至 Step 4。

Step3 记录用户自身对图片隐私信息的操作, 使用由 PKI 基础设施颁发的签名私钥对接收到的溯源记录信息 $\mathrm{Rec}_{\mathrm{owner}}$ 作为新溯源记录的一部分进行签名, 则有

$$\mathrm{Sig}_1=\mathrm{SIG}\left(\mathrm{Rec}_{\mathrm{owner}},S_1,O_1,\mathrm{OP}_1,\mathrm{CON}_1\right) \tag{8}$$

即溯源记录 Rec_1 的签名内容包括收到之前所有溯源记录 $\mathrm{Rec}_{\mathrm{owner}}$ 全部、Rec_1 除签名以外部分。

Step4 当签名验证不通过或隐私散列值不匹配时, 警告当前用户溯源记录已被破坏, 无法作为隐私侵犯行为判定的证据, 请勿继续转发。

3) 中间图片转发者 $\mathrm{forwarder}_i$ $(1<i\leq n)$ 执行与 2)中第一个图片转发者 $\mathrm{forwarder}_1$ 相同的处理流

程。其中，每个溯源记录 Rec_i 的签名内容包括溯源记录 Rec_{i-1} 的全部、Rec_i 除签名以外的部分，则有

$$\mathrm{Sig}_i = \mathrm{SIG}(\mathrm{Rec}_{\mathrm{owner}},\mathrm{Rec}_1,\cdots,\mathrm{Rec}_{i-1},S_i,O_i,\mathrm{OP}_i,\mathrm{CON}_i) \tag{9}$$

4) 当发生隐私泄露时，取证人员需对发生泄露节点的溯源记录信息进行逐层验签，以确保整条信息传播链上的信息未被篡改、伪造。

4.2.3　侵犯行为判定与溯源算法

确认整条传播链上溯源记录信息未被篡改或伪造后，取证人员需要对隐私侵犯行为进行判定。溯源取证判定与溯源流程如图 6 所示，具体步骤如下。

1) 判断当前节点溯源记录信息 Rec_i 中是否存在违反隐私侵犯行为标准 Pol（或延伸控制策略）的操作行为。

2) 当前节点的溯源记录 Rec_i 不存在隐私侵犯行为时，则对上一节点的溯源记录 Rec_{i-1} 进行判断，并重复执行步骤 1)，直到判断隐私侵犯行为终止。

4.3　安全性分析

4.3.1　隐私策略和溯源记录安全性分析

根据本文攻击模型，本节将对抵抗未授权攻击者、确保延伸控制策略不被非授权扩展和溯源记录不被篡改、伪造提供安全性分析。

当攻击来自未授权的攻击者 $\mathrm{attacker}_1$ 时，延伸控制系统的第二层加密算法可以阻挡攻击者获得隐私策略 PrA 的内容。如果延伸控制系统使用的公钥加密系统是安全的，则系统内外的攻击者 $\mathrm{attacker}_1$ 都无法获取隐私策略 PrA 的明文信息，亦不可通过篡改、伪造隐私策略 PrA 获取没有访问权限的隐私图片 p。

当攻击者 $\mathrm{attacker}_2$ 是系统内部诚实但好奇（HBC，honest-but-curious）的用户 User_i 时，该攻击者拥有部分操作权限 $\mathrm{PrA}_{i,1}$，并试图利用已有可赋予权限 $\mathrm{PrA}_{i,2}$ 与下一用户 User_{i+1} 合谋，通过赋予更高权限给 User_{i+1}，再转发回自己（此时用户 User_i 成为用户 User_{i+2}），从而提高自己的操作权限 $\mathrm{PrA}_{i+2,1}$。然而，由于延伸控制的约束条件 $\mathrm{PrA}_{i,2} \subseteq \mathrm{PrA}_{i,1}$，攻击者 $\mathrm{attacker}_2$ 可赋予的权限 $\mathrm{PrA}_{i,2}$ 是已有操作权限 $\mathrm{PrA}_{i,1}$ 的子集，因此不能获得更多权限。同时，攻击者 $\mathrm{attacker}_2$ 亦不可将可赋予权限 $\mathrm{PrA}_{i,2}$ 在操作权限 $\mathrm{PrA}_{i,1}$ 中的补集 $\mathrm{PrA}_{i,1} - \mathrm{PrA}_{i,2}$ 传播给下一用户 user_{i+1}。

此外，还有一类攻击者 $\mathrm{attacker}_3$ 知晓隐私侵犯行为判定标准 Pol 和溯源记录 Rec 的格式等背景知识，试图通过篡改、伪造判定标准 Pol 或溯源记录 Rec，以掩盖隐私侵犯行为或嫁祸他人。然而，嵌套签名算法要求用户 user_i 的签名内容 Rec_i 必须包括之前用户 $\mathrm{user}_{\mathrm{owner}} \sim \mathrm{user}_{i-1}$ 的签名信息 $\mathrm{SIG}(\mathrm{Rec}_{\mathrm{owner}},\mathrm{Rec}_1,\cdots,\mathrm{Rec}_{i-1},S_i,O_i,\mathrm{OP}_i,\mathrm{CON}_i)$，由于 $\mathrm{attacker}_3$ 不知道之前用户的私钥 $\mathrm{PriKey}_{\mathrm{owner}} \sim \mathrm{PriKey}_{i-1}$，因此无法伪造签名正确的溯源记录。当其他用户收到篡改图片时，即可利用溯源记录中用户的公钥 $\mathrm{PubKey}_{i-1} \sim \mathrm{PubKey}_{\mathrm{owner}}$ 进行逐层验签，发现信息传播链上的溯源记录中是否存在被篡改、伪造的情况，避免篡改图片继续传播。

4.3.2　图片隐私区域加密算法选择

本方案图片隐私区域的安全性主要依赖第一层加密算法保证，并且延伸控制系统所使用的加密算法可以根据不同的场景需求灵活更换。由于图片加密算法主要依赖终端设备或边缘服务器执行，因此本文挑选了一些轻量级的算法作为候选。此外，由于候选图片加密算法本身的安全证明已在相关文献中详细论述，本文便不再赘述。

当隐私图片的安全性要求较低时，可以选用高速的基于混淆映射的加密方案[26]来提高系统速度。此类算法将图片隐私区域划分为 $N \times N$ 个方格，再通过位置置乱的方式将不同方格、不同像素的位置进行混淆。该算法的优点在于加密时间与图片隐私区

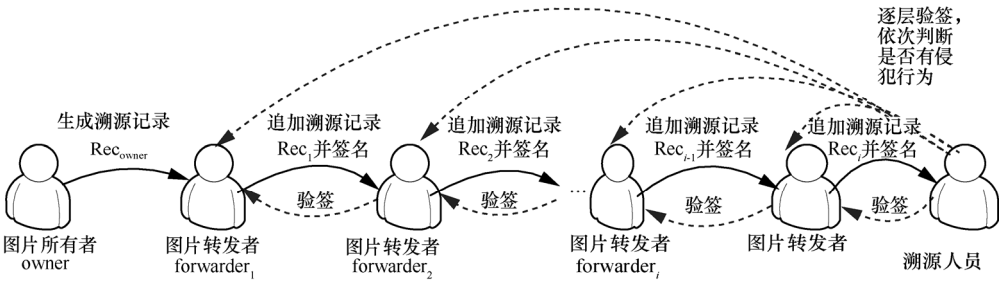


图 6　溯源取证判定与溯源流程

域大小无关（平均耗时约 3.1 s），仅与方格数目有关。但是该算法并没有改变图片的像素值，如果攻击者拥有一定的背景知识，比如通过图片公开区域得知该图片的背景信息，从而找到未加密图片所在的候选集，即可根据统计特征分析判断出加密图片对应的原始内容。

为了更好地达到保护隐私区域的效果，本文从现有工作中选用了一种安全性与时间消耗较为均衡的对称加密方案[25]来保护隐私。该方案加密时间与图片隐私区域的大小正相关（如表 2 所示），由于图片中的隐私区域通常较小，因此该方案在日常图片分享中更为实用。

表 2 图片区域加解密时间消耗

图片大小	低强度	中强度	高强度
200 像素×150 像素	117.79 ms	125.88 ms	142.68 ms
700 像素×525 像素	148.23 ms	158.31 ms	174.53 ms
1 200 像素×900 像素	247.37 ms	264.13 ms	299.61 ms
1 700 像素×1 275 像素	2.92 s	3.14 s	3.54 s
2 400 像素×1 800 像素	4.90 s	5.24 s	5.87 s
2 800 像素×2 100 像素	8.66 s	9.27 s	10.57 s
3 200 像素×2 400 像素	12.52 s	14.32 s	16.23 s
4 032 像素×3 024 像素	23.87 s	25.71 s	29.20 s

5 实验及分析

为测试本文提出的隐私图片分享框架，本章实现了延伸控制和溯源取证方案的原型系统，包括一个 Android 插件和一个服务器，其中，Android 插件在图片分享中扮演第三方的角色，且不受限于任何确定的图片分享社交网络；服务器负责图片区域的加解密及分配和管理密钥工作。

5.1 延伸控制效果评估

为测试延伸控制系统的实际效果，在一台 OnePlus 3T 智能手机（手机配置为 2.15 GHz CPU，6 GB RAM）上进行测试，并使用一台 ThinkPad T430U 作为 CA 服务器。为更好地了解用户的分享行为和隐私偏好，本文开展了一项用户调研，并邀请了 27 名志愿者，请他们在 2 周内使用延伸控制系统进行图片分享并反馈他们是否分享图片的理由。实验从志愿者的反馈中共收集了 1 722 张图片和 647 条隐私策略。

5.1.1 延伸控制原型系统

当用户想要通过延伸控制系统上传一张图片时，需要选择隐私区域并为每个隐私区域分配密钥。之后，为传播链上后续用户分配延伸控制策略，约束用户可以做什么及可以给后续用户分配什么样的权限。图 7 展示了延伸控制系统的用户界面。延伸控制系统可以兼容现有社交网络的访问控制机制，并不需要其他额外的修改工作。传统的访问控制策略可以很容易地加入延伸控制系统的访问控制条件中。

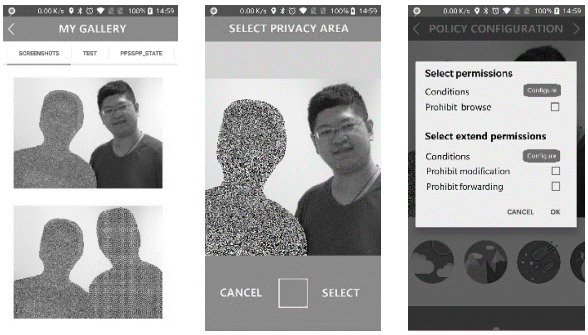


图 7 延伸控制系统界面

5.1.2 性能评估

实验从志愿者图片中随机选取了 100 张图片，并利用延伸控制系统对图片进行处理。整个流程（不包括加解密时间）平均每张图片仅耗时 45 ms。如表 2 所示，图片的加解密时间与图片加密区域的大小密切相关。此外，加密强度参数同样会影响加密时间消耗。需要指出的是，第二层的加密时间相较于第一层的加密时间是可以忽略的。平均而言，第二层加密与解密时间分别仅需要 47.63 ms 和 41.35 ms。

5.1.3 用户评估

在本实验中，很多志愿者改变了他们最初的分享策略，并且更严格地限制了图片的分享行为。在部分志愿者的反馈中发现，一些延伸控制策略，比如最长展示时间限制、转发次数限制等可以有效地避免图片隐私信息的广泛传播。这些发现表明，用户并不愿意让他们的图片被无限制的转发。因此，延伸控制系统对图片隐私信息跨社交网络传播进行控制和溯源是有效和有必要的。

5.2 溯源取证效果评估

为评估图片隐私信息溯源取证方案的有效性和效率，本章实现了一个溯源取证系统原型，如图 8 所示，并从功能和性能 2 个方面对溯源取证系统进行评估。本实验邀请曾经参与延伸控制系统实验的志愿者进行了为期 2 周的实验。在溯源取证系统实验过程中，暂时取消了延伸控制机制， 而将延伸

图 8　溯源取证系统管理界面

控制策略作为隐私侵犯行为判定标准。由于溯源取证系统对用户透明，志愿者们在使用过程中并不需要直接与溯源取证系统交互，在使用系统 2 周后，实验组获得了 134 条隐私侵犯行为的测试数据。

5.2.1　功能正确性评估

在本例中，选取一张私人聚会的隐私图片，Alice 在图片中标注了 2 个隐私区域，用户的“脸部区域”和“首饰所在的图像区域”。“脸部区域”在图片中的像素坐标分别为(354, 234; 410, 290)，“首饰所在的图像区域”在图片中的坐标为(467, 237; 497, 302)。

假设 Alice 将图片中的隐私区域加密转发给了 Bob，同时设置希望该“首饰所在的图像区域”仅在同学范围内分享，且不允许其他用户再对“脸部区域”进行马赛克、模糊处理。Bob 将“首饰所在的图像区域”转发给同学范围中的 Carol 和同学范围外的 David，而 Carol 对图片中的“脸部区域”进行了马赛克处理。

溯源记录信息将记录以下信息。

“溯源记录信息 001；操作主体：Alice；操作类型：标记、加密；操作时间：2018-03-04 20:30:43”。

“溯源记录信息 002；操作主体：Alice；操作类型：转发（Bob）；操作时间：2018-03-04 20:42:41”。

“溯源记录信息 003；操作主体：Bob；操作类型：查看（脸部、首饰）、转发（Carol、David）；操作时间：2018-03-04 21:42:23”。

“溯源记录信息 004；操作主体：Carol；操作类型：查看（脸部、首饰）；操作时间：2018-03-05 09:12:51”。

“溯源记录信息 005；操作主体：Carol；操作类型：马赛克（脸部区域）；操作时间：2018-03-05 11:32:42”。

在另一条传播路径上存在以下信息。

“溯源记录信息 004；操作主体：David；操作类型：查看（脸部、首饰）；操作时间：2018-03-05 08:07:14”。

在隐私侵犯行为发生后，实验人员在查询过程中，得到以下隐私侵犯行为判定结果。

“溯源记录 004；操作主体：David；操作类型：查看；操作时间：2018-03-05 08:07:14”超出“首饰所在的图像区域”查看权限的访问限制条件“同学范围”，判定为隐私侵犯行为。

“溯源记录 005；操作主体：Carol；操作类型：马赛克（脸部区域）；操作时间：2018-03-05 11:32:42”超出“脸部区域”“禁止马赛克、模糊”的隐私处理权限，判定为隐私侵犯行为。

5.2.2　性能评估

溯源取证方案记录函数的时间消耗集成进延伸控制机制，平均每张图片增加功耗 14 ms（不包含签名验签时间）。溯源记录签名和验签的时间与溯源链的长度密切相关。为解社交网络中信息传播链的最大长度，李彪[31]调研了 6 025 条高转发微博，平均每条微博被转发 1 836 次，总转发次数为 1 108 万次，其中传播链最大长度为 13 次，平均长度为 6 次。此外，路由协议 RIP 则认为 16 跳连接为不可达。如图 9 所示，本实验测试了溯源记录在最差情况下的签名和验签时间。假设每条溯源记录信息包含 50 B 的内容和 64 B 的签名值，在 20 次交换情况下的签名时间仅为 18.09 ms。

5.3　讨论

1) 录屏攻击

在延伸控制系统中，为保护图片中高敏感区域不被其他用户获得，图片在通过插件导出系统时将会被加密。然而，一些 HBC 用户仍然希望拍屏或

录屏的方式存储图片的明文副本。这种类型的攻击并没有被考虑在本文的工作中, 因为可以将文献[32]方案很容易地集成到延伸控制系统中。

2) 策略嵌入与隐写术

现有技术中存在大量利用隐写术将信息嵌入图片像素信息的方案，本文未采用隐写术来嵌入延伸控制策略和溯源记录信息的原因在于，图片传播过程中一些对图片像素的操作，如剪裁、缩放和滤镜会破坏嵌入像素中的策略。而 EXIF 等图片描述信息在很多情况下可以避免传播过程中的处理行为破坏。

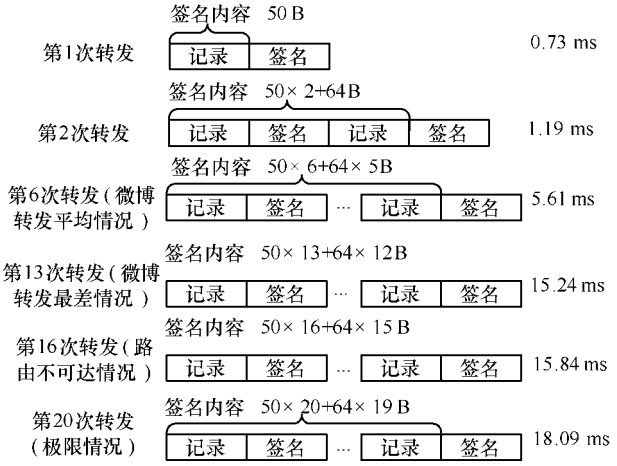


图 9 嵌套签名方案签名内容与消耗时间

6 结束语

本文针对图片社交网络中的转发隐私泄露问题，提出了一个跨社交网络的隐私图片分享框架。该框架可以辅助用户限制在传播链上后续用户的操作和追加策略范围。首先，该框架可以在用户发布图片前对隐私区域进行加密，并将访问控制和延伸控制策略绑定到图片上，在随图片流转过程中不会干扰图片在社交网络中的正常显示。因此，即使在不同的社交网络中，延伸控制系统依然可以根据策略保护用户的隐私图片。在此基础上，本文将跨社交网络的隐私图片分享框架运用到溯源取证中，为隐私侵犯行为的发现提供溯源记录信息。最后，本文实现了隐私图片分享原型系统，并在一组真实的实验数据上进行测试，实验结果进一步说明了框架的有效性和效率。

参考文献：

[1] HU H, AHN G J, JORGENSEN J. Multiparty access control for online social networks: model and mechanisms[J]. IEEE Transactions on Knowledge and Data Engineering, 2013, 25(7): 1614-1627.

[2] ILIA P, POLAKIS I, ATHANASOPOULOS E, et al. Face/off: preventing privacy leakage from photos in social networks[C]//The 22nd ACM SIGSAC Conference on Computer and Communications Security. 2015: 781-792.

[3] VISHWAMITRA N, LI Y, WANG K, et al. Towards PII-based multiparty access control for photo sharing in online social networks[C]//The 22nd ACM on Symposium on Access Control Models and Technologies.2017: 155-166.

[4] XU K, GUO Y, GUO L, et al. My privacy my decision: control of photo sharing on online social networks[J]. IEEE Transactions on Dependable and Secure Computing, 2017, 14(2): 199-210.

[5] LI F, LI Z, HAN W, et al. Cyberspace-oriented access control: a cyberspace characteristics based model and its policies[J]. IEEE Internet of Things Journal, 2018, 6(2): 1471-1483.

[6] LI F, SUN Z, NIU B, et al. HideMe: privacy-preserving photo sharing on social networks[C]//The 38th IEEE International Conference on Computer Communications. 2019: 154-162.

[7] RA M R, GOVINDAN R, ORTEGA A. P3: toward privacy-preserving photo sharing[C]//The 10th USENIX Symposium on Networked Systems Design and Implementation. USENIX, 2013: 515-528.

[8] ZHANG L, JUNG T, LIU C, et al. Pop: privacy-preserving outsourced photo sharing and searching for mobile devices[C]//The 35th IEEE International Conference on Distributed Computing Systems. 2015: 308-317.

[9] HE J, LIU B, KONG D, et al. Puppies: transformation-supported personalized privacy preserving partial image sharing[C]//The 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks.2016: 359-370.

[10] SUN W, ZHOU J, ZHU S, et al. Robust privacy-preserving image sharing over online social networks (OSNs)[J]. ACM Transactions on Multimedia Computing, Communications, and Applications, 2018, 14(1): 14.

[11] 李晖. 隐私计算—面向隐私保护的新型计算[J]. 信息通信技术, 2018, 12(6): 4-6.
LI H. Privacy computing: a new computing model for privacy preserving[J]. Information and Communications Technologies, 2018, 12(6): 4-6.

[12] KARJOTH G, SCHUNTER M, WAIDNER M. Platform for enterprise privacy practices: privacy-enabled management of customer data[C]//Springer International Workshop on Privacy Enhancing Technologies.2002: 69-84.

[13] 薛见新, 申德荣, 寇月, 等. 面向数据融合的半环溯源计算方法[J]. 计算机研究与发展, 2016, 53(2): 316-325.
XUE J X, SHEN D R, KOU Y, et al. Semiring provenance for data fusion[J]. Journal of Computer Research and Development, 2016, 53(2): 316-325.

[14] 王梁, 周光焱, 王黎维, 等. 不确定关系数据属性级溯源表示与概率计算[J]. 软件学报, 2014, 25(4): 863-879.
WANG L, ZHOU G Y, WANG L W, et al. Attribute level lineage and probabilistic computation of uncertain data[J]. Journal of Software, 2014, 25(4): 863-879.

[15] SUN L, PARK J, NGUYEN D, et al. A provenance-aware access control framework with typed provenance[J]. IEEE Transactions on Dependable and Secure Computing, 2016, 13(4): 411-423.

[16] 张聿博, 张锡哲, 张斌. 面向社交网络信息源定位的观察点部署方

法[J]. 软件学报, 2014, 25(12): 2837-2851.
ZHANG Y B, ZHANG X Z, ZHANG B. Observer deployment method for locating the information source in social network[J]. Journal of Software, 2014, 25(12): 2837−2851.

[17] 付安民, 秦宁元, 宋建业, 等. 云端多管理者群组共享数据中具有隐私保护的公开审计方案[J]. 计算机研究与发展, 2015, 52(10): 2353-2362.
FU A M, QIN N Y, SONG J Y, et al. Privacy-preserving public auditing for multiple managers shared data in the cloud[J]. Journal of Computer Research and Development, 2015, 52(10): 2353-2362.

[18] SUCH J M, CRIADO N. Resolving multi-party privacy conflicts in social media[J]. IEEE Transactions on Knowledge and Data Engineering, 2016, 28(7): 1851-1863.

[19] XU Y, PRICE T, FRAHM J M, et al. Virtual U: defeating face liveness detection by building virtual models from your public photos[C]//The 25th USENIX Security Symposium. 2016: 497-512.

[20] FOGUES R L, MURUKANNAIAH P K, SUCH J M, et al. Sharing policies in multiuser privacy scenarios: Incorporating context, preferences, and arguments in decision making[J]. ACM Transactions on Computer-Human Interaction, 2017, 24(1): 5.

[21] LI F, SUN Z, NIU B, et al. SRIM scheme: an impression-management scheme for privacy-aware photo-sharing users[J]. Engineering, 2018, 4(1): 85-93.

[22] YUAN X, WANG X, WANG C, et al. Enabling privacy-preserving image-centric social discovery[C]//The 34th IEEE International Conference on Distributed Computing Systems. IEEE, 2014: 198-207.

[23] HE J, LIU B, BAO X, et al. On privacy preserving partial image sharing[C]// The 35th IEEE International Conference on. Distributed Computing Systems. IEEE, 2015: 758-759.

[24] FERREIRA B, RODRIGUES J, LEITAO J, et al. Privacy-preserving content-based image retrieval in the cloud[C]//The 34th IEEE Symposium on Reliable Distributed Systems. IEEE, 2015: 11-20.

[25] YUAN L, KORSHUNOV P, EBRAHIMI T. Secure JPEG scrambling enabling privacy in photo sharing[C]//The 11th IEEE International Conference and Workshops on Automatic Face and Gesture Recognition. IEEE, 2015, 4: 1-6.

[26] NOURIAN A, MAHESWARAN M. Privacy aware image template matching in clouds using ambient data[J]. The Journal of Supercomputing, 2013, 66(2): 1049-1070.

[27] PEARSON S, MONT M C, KOUNGA G. Enhancing accountability in the cloud via sticky policies[C]//Springer FTRA International Conference on Secure and Trust Computing, Data Management, and Application.2011: 146-155.

[28] SPYRA G, BUCHANAN W J, EKONOMOU E. Sticky policies approach within cloud computing[J]. Elsevier Computers & Security, 2017, 70: 366–375.

[29] PARK J, NGUYEN D, SANDHU R. A provenance-based access control model[C]//The 10th Annual International Conference on Privacy, Security and Trust.2012: 137-144.

[30] BATES A M, TIAN D, BUTLER K R B, et al. Trustworthy whole-system provenance for the Linux kernel[C]//The 24th USENIX security symposium. USENIX, 2015: 319-334.

[31] 李彪. 微博中热点话题的内容特质及传播机制研究——基于新浪微博 6 025 条高转发微博的数据挖掘分析[J]. 中国人民大学学报, 2013, 27(5): 10-17.
LI B. Research on content characteristics and communication mechanism of hot topics in weibo--data mining and analysis based on sina weibo 6025 highly retweeted microblogs[J]. Journal of Renmin University of China, 2013, 27(5): 10-17.

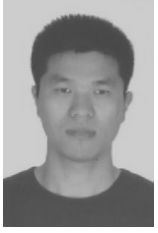
[32] ZHANG L, BO C, HOU J, et al. Kaleido: you can watch it but cannot record it[C]//The 21st ACM Annual International Conference on Mobile Computing and Networking .2015: 372-385.

[作者简介]

李凤华（1966− ），男，湖北浠水人，博士，中国科学院信息工程研究所研究员、博士生导师，主要研究方向为网络与系统安全、信息保护、隐私计算。

孙哲（1987− ），男，安徽安庆人，中国科学院信息工程研究所博士生，主要研究方向为信息保护、隐私计算。

牛犇（1984− ），男，陕西西安人，博士，中国科学院信息工程研究所副研究员，主要研究方向为网络安全、隐私计算。



曹进（1985− ），男，陕西西安人，博士，西安电子科技大学副教授、硕士生导师，主要研究方向为应用密码学、安全协议分析、无线网络安全。

李晖（1968− ），男，河南灵宝人，博士，西安电子科技大学教授、博士生导师，主要研究方向为密码学、无线网络安全、云计算安全、信息论与编码理论。