面向版式文档的细粒度隐私操作控制方法

尹沛捷[1,2]，李凤华[1,2]，牛犇[1]，罗海洋[1,2]，邝彬[1,2]，张玲翠[1]
（1. 中国科学院信息工程研究所，北京 100085；2. 中国科学院大学网络空间安全学院，北京 100049）

摘 要：针对隐私信息频繁交换场景下不可控转发导致的隐私信息泄露问题，提出了一种面向版式文档的细粒度隐私操作控制方法，可实现隐私信息在分享过程中按分享者的要求进行差异化细粒度的隐私操作控制。对接收到的多模态版式文档提取已有隐私操作控制策略，结合当前分享者使用属性、接收者隐私保护能力等因素，迭代生成隐私操作控制策略，并给出了抽象化的控制策略生成算法框架；基于迭代隐私操作控制策略，结合具体操作场景，对不同模态的信息分量进行差异化脱敏控制、交换边界控制和本地使用控制，并给出了抽象化的隐私操作控制算法框架。实验开发了 OFD 的隐私操作控制前后台原型系统，并对上述方法进行了验证，在即时通信系统中实现了基于好友关系的迭代隐私操作控制策略生成与传递，以及 OFD 的差异化脱敏控制、交换边界控制和本地使用控制。

关键词：隐私操作控制；迭代；版式文档
中图分类号：TN92
文献标志码：A
DOI: 10.11959/j.issn.1000−436x.2023083

Fine-grained privacy operation control method for layout documents

YIN Peijie[1,2], LI Fenghua[1,2], NIU Ben[1], LUO Haiyang[1,2], KUANG Bin[1,2], ZHANG Lingcui[1]
1. Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100085, China
2. School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China

Abstract: In view of the problem of privacy information disclosure caused by uncontrolled forwarding in the context of frequent exchange of privacy information, a fine-grained privacy operation control method for layout documents was proposed, which could achieve differentiated fine-grained privacy operation control according to the requirements of the sharer during the sharing process of privacy information. For the received multimodal layout document, the existing privacy operation control strategy was extracted, which combined the current sharer's use attribute and the receiver's privacy protection ability and other factors. The privacy operation control strategy was generated iteratively, and an abstract control strategy generation algorithm framework was given. Based on the iterative privacy operation control strategy and combined with specific operation scenarios, the differentiated data-masking control, exchange boundary control and local use control were carried out for different modes of information components, and the abstract privacy operation control algorithm framework was given. A prototype system for privacy operation control of OFD (open fixed-layout document) was developed to verify the above algorithms. The generation and delivery of iterative privacy operation control strategy based on friendship, as well as the differential data-masking control, exchange boundary control and local use control of OFD were implemented in the instant messaging system.

Keywords: privacy operation control, iteration, layout document

收稿日期：2023−01−31；**修回日期：**2023−03−17
通信作者：张玲翠，zhanglingcui@iie.ac.cn
基金项目：国家重点研发计划基金资助项目（No.2021YFB3101301）；国家自然科学基金资助项目（No.61932015）；国家社科基金重大项目（No.22&ZD147）
Foundation Items: The National Key Research and Development Program of China (No.2021YFB3101301), The National Natural Science Foundation of China (No.61932015), Major Programs of the National Social Science Foundation of China (No.22&ZD147)

0　引言

随着信息技术、网络技术的不断发展，万物智慧互联、信息泛在共享成为未来网络发展趋势。在社交媒体、在线办公等各种新应用模式的带动下，版式文档在不同用户分组、不同即时通信系统内等广泛交换已成为常态。近年来，隐私泄露事件层出不穷，引发众多关注。

用户一旦与他人分享文档，任何一个接收者都可以对其进行浏览、转发、修改等处理。后续分享者经常会违背信息的隐私操作控制要求，还会不受限制地交换分享给其他人。以微信为代表的即时通信系统会基于每一个分享者自身的好友名录交换信息。如图 1 所示，分享者 u_{11} 向自己的好友分享信息，其分属于多个朋友圈。首次分享时，分享者 u_{11} 向自己所有的好友（u_{12}、u_{13}、u_{14} 和 u_{15}）分享信息（如图 1 中实线箭头表示）。其中，u_{14} 和 u_{15} 这 2 个好友收到信息后，又向其分别所属的其他朋友圈进行迭代分享（如图 1 中虚线箭头表示），就会将信息传递给 u_{21}、u_{22} 和 u_{23} 这 3 个接收者。

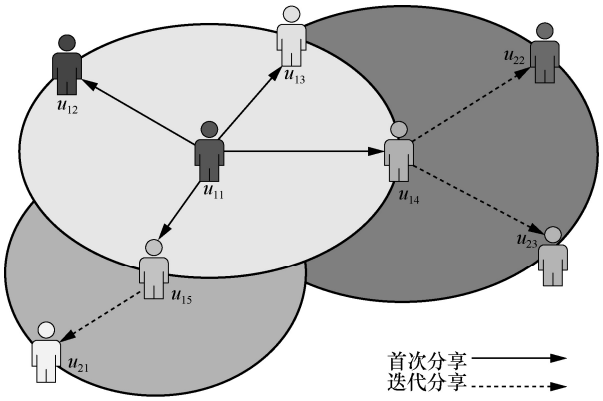

图 1　迭代信息分享场景

对上述迭代信息分享场景进行抽象建模，得到如图 2 所示的隐私操作控制关联关系及传递。Alice（可以将她抽象定义为第 i 次分享的信息来源，记为 S_{i-1}）想将一个版式文档通过即时通信系统发送给朋友 Bob 和 Cindy（可以将他们抽象定义为第 i 次分享时的当前信息持有者，标记为 S_i）；Cindy 在查看、编辑后，又将该版式文档发送给自己的朋友 Dale 和 Eric（可以将他们抽象定义为第 i 次分享时的信息接收者，标记为 S_{i+1}）。Alice 的诉求是只想分享给自己的朋友，Bob 和 Cindy 是 Alice 的朋友，Dale 和 Eric 是 Cindy 的朋友，却不一定是 Alice 的朋友。Cindy 再分享的行为对 Alice 来说是不可控的，甚至，Alice 如果不希望分享给 Dale 和 Eric，那么 Cindy 的再分享就违背了 Alice 最初的分享诉求。将分享进行归纳如下：在信息分享过程中，S_{i-1} 将信息分享给 S_i，S_i 再分享给 S_{i+1}，信息要根据三者的传递关系和各自接收者的不同，逐渐减少信息所含内容。

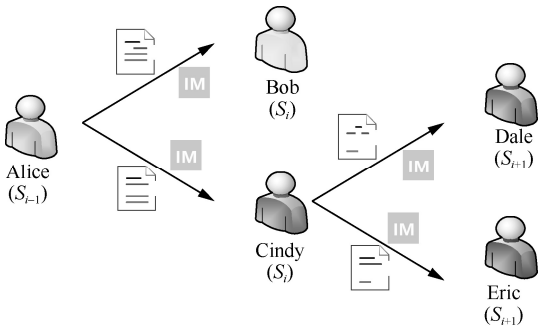

图 2　迭代信息分享的隐私操作控制关联关系及传递

为解决在交换、处理等分享过程中隐私信息不可控的多次转发所带来的隐私泄露问题，研究者将隐私保护与访问控制技术相结合[1-3]，围绕隐私操作控制策略生成和隐私操作控制 2 个方面提出了不同的解决方案。在隐私操作控制策略生成方面，分别基于风险[4-5]和时间[3,6-7]等要素对控制策略进行动态调整，同时将策略与信息进行关联，确保控制策略随信息流转[8-10]。在隐私操作控制中的脱敏操作控制方面，根据算法的保护效果选择脱敏算法，从而实现细粒度的脱敏操作控制[11-12]；在隐私操作控制中的交换边界控制方面，构建信息流动最小管控单元，对信息流动进行细粒度控制[13-14]。但上述方法不能根据访问场景和用户意图调整隐私操作控制权限，且未能将动态调整权限的策略与信息绑定来实现约束信息后续的脱敏、交换和使用等隐私操作控制。

针对上述问题，本文从信息迭代分享的应用需求出发，提出了一种面向版式文档的细粒度隐私操作控制方法。具体地，该方法包括能够提取所有分享者要求的迭代隐私操作控制策略生成方法和能够执行该策略的版式文档隐私操作控制方法，并在即时通信系统内信息交换过程中进行验证。根据迭代隐私操作控制策略，对版式文档的不同模态对象选择合适的脱敏算法进行差异化脱敏控制、交换边界控制和本地使用控制，再将隐私操作控制策略嵌入脱敏后的版式文档传递给接收者，实现细粒度隐

私操作控制，限制其脱敏、交换和使用。本文主要的贡献点如下。

1) 提出一种迭代隐私操作控制策略生成方法。该方法基于前序分享者的隐私操作控制要求，结合当前分享者的使用属性、接收者的隐私保护能力等因素，迭代生成隐私操作控制策略，并以版式文档为例说明该方法的应用。

2) 提出一种版式文档隐私操作控制方法。该方法基于迭代隐私操作控制策略，结合具体操作场景，对信息分量进行具体的隐私操作控制。本文对隐私操作控制进行抽象，并给出版式文档的差异化脱敏、交换边界控制和本地使用控制3种典型操作控制模式，以此说明该方法的应用。

3) 开发OFD（open fixed-layout document）的隐私操作控制前后台原型系统。该系统可以实现基于好友关系的OFD迭代隐私操作控制策略生成与传递，以及OFD的差异化脱敏操作控制、交换边界控制和本地使用控制3种典型操作控制模式。

1 相关工作

本节从控制策略生成和隐私操作控制2个方面对现有相关解决方法予以梳理。

1.1 控制策略生成

大多数已有控制策略生成方法在将信息分享给他人后，无法更新本地策略并控制他人在同一场合或其他场合将信息再次分享。然而，信息不可控的多次分享可能被用于挖掘更多的隐私，严重威胁隐私保护。信息分享的控制过程离不开在传递策略的过程中对其进行的不断调整。Karjoth 等[8]提出了一种称为“粘性策略”的跨系统访问控制方法，将访问控制策略绑定到原始信息上，从而解决跨系统交换的问题。Pearson 等[9]提出了一种实用的跨云隐私保护框架，通过将隐私信息与安全策略绑定实现隐私信息的跨云控制。Spyra 等[10]使用加密机制将策略与数据相关联，并对策略进行属性编码和匿名化处理以防止被恶意利用，为全生命周期内数据访问控制提供支持。这些研究大多关注于单个策略的延伸控制，未考虑将策略不断补充修改而带来的迭代控制问题。

同时，策略在信息分享的过程中还应进行权限动态自动调整。在基于风险的权限调整方案中，首先依据用户场景，定义数据访问所面临的风险指标；然后计算权限调整前和调整后的风险，当风险小于预定阈值时，可调整访问权限[4-5]。在基于时间的权限调整方案中，首先设定用户仅在某个时间域内对数据的访问权限，在系统执行过程中，一旦超出预定时间域，系统自动检测并撤销或调整已分配权限[3,6]。此外，Yan 等[7]将上下文感知的信任与声誉评估集成到加密系统，提出了基于信任的访问控制方案，支持访问权限随策略变化而动态调整。综上，现有访问权限的调整主要基于风险和时间等要素，尚未做到权限随访问场景变化而自适应调整。

李凤华等[15]在隐私计算理论中首次提出迭代控制，其核心思想是在脱敏、控制、使用等过程中对跨系统交换场景下的个人信息实施多次控制。针对图片分享，他们又提出了将控制策略与信息一同流转交换的保护策略，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[16-18]，并在文献[19]中设计了一种基于图片分享场景下信息的隐私保护策略生成方法HideMe。

1.2 隐私操作控制

现有的隐私操作控制方法种类繁多，包括对文档进行隐私脱敏操作控制、对文档出入域进行边界控制等。在脱敏操作控制方面，需根据情况的不同选择合适的脱敏算法。Niu 等[11]提出了一种位置隐私保护场景下的算法选择框架，该框架结合用户自身偏好，综合考虑脱敏算法资源开销、保护效果与影响等因素，动态筛选出符合用户脱敏需求和实时资源情况的脱敏算法。Chen 等[12]提出了一种隐私保护数据分类的随机调整旋转扰动的方法，综合考虑了数据隐私丢失和信息丢失之间的平衡关系，对数据可用性和安全性进行控制。此类研究相对较少，大多研究工作专注于某一具体场景，且对脱敏算法的推荐往往只涵盖少部分经典算法，尚未形成普适框架。

在边界控制方面，Wang 等[13-14]提出了保障数据收集、管理和处理合规的隐私警戒模型PrivGuard[14]，利用数据、用于描述该数据的元数据，以及限制该数据处理方式的策略等，构成其模型中最小的管控单元，并利用可随信息流动的策略实现对信息流动的管控，但该工作未考虑策略动态调整，且忽略了迭代控制。李凤华等[20]提出了面向网络空间的访问控制（CoAC, cyberspace-oriented

access control）模型，利用资源传播链和网络传播链对个人信息在跨系统跨生态圈的流转进行管理和控制。但该模型是主体对客体在不同流转过程中知悉范围的控制，不包含对交换后数据的脱敏，也未强调策略随数据的绑定与流转。

以上方法中的隐私操作控制多数只是一次性的，缺乏统一的全生命周期角度的连贯性，隐私性无法得到有效保障。一次隐私操作控制之后无法对后续交换进行约束，缺少一种能够适配于即时通信系统内交换共享的细粒度隐私操作控制方法，无法满足隐私信息在交换过程中多次转发所面临的多次隐私操作控制诉求。

2　面向版式文档的隐私操作控制

本节首先介绍面向版式文档的细粒度隐私操作控制方法的背景和架构，然后详细描述了所提方法的核心迭代隐私操作策略生成、差异化隐私操作控制。本文中所有符号及其含义如表 1 所示。

2.1　要素抽象

在信息分享过程中，不同的参与者会对所收到的信息产生不同的隐私操作控制要求，基于此可对该信息进行不同粒度的操作控制。为了在分享过程中确保隐私操作控制要求的有效实施，需将这些隐私操作控制要求以隐私操作控制策略的方式嵌入原始信息中，与信息一起流转分享。

在此背景下，本文提出一种面向版式文档的细粒度隐私操作控制方法，将即时通信系统内版式文档的分享抽象为如下 3 个要素。

版式文档 X：交换过程中被分享的本文方法研究对象及其相关属性。

分享者 S：信息分享过程中所有参与者的统称，分享者可以是信息分享发起者 Alice，也可以是接收到信息后分享或可能分享给他人的人，如 Bob、Cindy 等。由于信息的分享交换是借助于即时通信系统等媒介，所有的分享者之间会存在一定的关联关系，比如家人、朋友、同事等。每个分享者都可以根据自身的使用属性设置脱敏、交换和使用约束，比如在什么情况下需要脱敏什么内容，或者交换给多少人后需要降低多少的敏感度等。当系统将这些设置提取之后，会生成隐私操作控制策略 $\mathbb{P}$，并基于此执行相应的隐私操作控制。

表 1　本文中所有符号及其含义

符号	含义
$X=\{X_1, X_2, \cdots, X_k, \cdots, X_n\}$	版式文档 X 及其信息分量 X_k
$X_k=\langle c, A, \Gamma, \Omega, \Psi, \mathbb{P}\rangle$	信息分量 X_k 的组成内容
c	信息分量的内容
A	隐私属性向量（量化隐私信息分量及分量组合的保护程度）
Γ	广义定位信息集合
Ω	审计控制信息集合（流转过程中的主客体信息和被执行的操作记录）
Ψ	共享控制操作集合（信息分量及其组合可被执行的操作）
$\mathbb{P}$	隐私操作控制策略集合
$X_k.\mathbb{P}$	版式文档信息分量 X_k 的当前迭代隐私操作控制策略集合
$X_k.\mathbb{P}_{exist}$	接收到版式文档时信息分量 X_k 已有的迭代隐私操作控制策略集合
$X_k.P_j$	信息分量 X_k 的第 j 条隐私操作控制策略
$X_k.P_j'$	信息分量 X_k 的第 j 条隐私操作控制策略调整后的策略
S_{i-1}, S_i, S_{i+1}	前一分享者，当前分享者，接收者
X'	脱敏后的版式文档
G_{pic}	图片脱敏算法库
G_{wds}	文字脱敏算法库
t	策略调整动作
para.opt	操作控制目的
para.opt.dataMasking	操作控制目的为脱敏操作控制的标志位
para.opt.broadControl	操作控制目的为交换边界控制的标志位
para.opt.localControl	操作控制目的为本地使用控制的标志位
para.opt.direction	交换方向，比如传出、传入等
para.opt.mod	交换模式，比如查看该信息的人员、方式、位置、设备（终端、后台服务器）、时间等
OP_{bc}	交换边界控制判断结果
OP_{lc}	本地使用控制判断结果
f_1	策略调整虚函数
f_2/f_5	图片/文字脱敏算法选择虚函数
f_3/f_6	图片/文字交换边界控制虚函数
f_4/f_7	图片/文字本地使用控制虚函数
g_1/g_2	所选出的对图片/文字的脱敏算法
Attr(S_i)	当前分享者使用属性
Attr.scene	场景
Attr.desire	操作要求
Ability(S_{i+1})	接收者隐私保护能力（接收者 S_{i+1} 的硬件和软件保护能力，比如硬件防护能力包括但不限于内存运行能力、CPU 运行能力、防火墙、隔离网关等，软件防护能力包括但不限于恶意监听者查杀软件、流量监控能力等）
Ability.hardware	硬件防护能力

隐私操作控制策略集合 $\mathbb{P}$：对某个信息进行脱敏、交换和使用等约束的策略集合，系统将其嵌入信息中并随之分享。当信息被分享时，隐私操作控制策略会约束后续的分享者如何进行隐私操作，包括如何脱敏、如何使用等。

2.2　细粒度隐私操作控制方法

本文方法在不可预测信息分享过程的情况下，基于隐私操作控制策略，指导信息在分享中按照已分享者的要求进行脱敏、交换和使用，接收到该文档的接收者只能按照上一分享者要求的方式操作他们可操作的部分内容，尽可能减少信息泄露。

本文方法的抽象流程如图 3 所示。

步骤 1　初始化。接收到版式文档 X 后，已知 X 由 n 个信息分量组成，即 $X=\{X_1, X_2, \cdots, X_k, \cdots, X_n\}$，每个信息分量 X_k 的组成内容是 $X_k=\langle c, A, \Gamma, \Omega, \Psi, \mathbb{P}\rangle$ [21]，提取已有的隐私操作控制策略 $X.\mathbb{P}_{\text{exist}}$，信息分量的切分不在本文讨论范围，实现中可借用现有的自然语言处理方法。

步骤 2　迭代隐私操作控制策略生成。针对信息分量 X_k，依据已有的隐私操作控制策略 $X_k.\mathbb{P}_{\text{exist}}$，并与当前分享者 S_i 使用属性 Attr(S_i)、接收者 S_{i+1} 的隐私保护能力 Ability(S_{i+1})等因素综合分析，迭代生成信息分量 X_k 的第 j 条隐私操作控制策略 $X_k.P_j$ 调整后的策略 $X_k.P_j'$ 和策略调整动作 t。

步骤 3　版式文档差异化隐私操作控制。针对每一个信息分量 X_k，可执行差异化脱敏操作控制、交换边界控制和本地使用控制中的一个或多个操作。以隐私操作控制策略 $X.\mathbb{P}$ 为基础，针对版式文档的不同模态（即数据格式，常见模态有图像、文字等）及保护策略进行差异化脱敏控制；针对当前分享者的分享方向判断版式文档需要部分过滤、全部过滤和放行等的交换边界控制；针对本地设备模式判断文档如何显示、复制、粘贴等的本地使用控制。

2.2.1　*初始化*

初始化主要包含提取已有隐私操作控制策略 $X.\mathbb{P}_{\text{exist}}$、进行身份认证等子步骤。首先，根据信息是否为首次分享将分享者分为首次分享者和迭代分享者。首次分享者可查看文档全部内容直接进入步骤 2，而迭代分享者则需先进行初始化操作。由于当前分享者从前一分享者处收到版式文档 X 时是无法直接查看版式文档 X 内容的，因此分享者 S_i 首先用私钥对文档进行外层解密，提取出已有隐私操作控制策略 $X.\mathbb{P}_{\text{exist}}$ 和内容仍为密文的版式文档 X；然后将版式文档 X、分享者 S_i 和提取出的已有隐私操作控制策略 $X.\mathbb{P}_{\text{exist}}$ 构成身份认证请求 req = (X, S_i, $X.\mathbb{P}_{\text{exist}}$)，判断该分享者 S_i 是否可以查看版式文档 X 内容。如果通过身份认证，则可获得解密版式文档 X 的密钥，进行内层解密后可以正常查看该文档；否则，该分享者 S_i 会被告知不具备查看

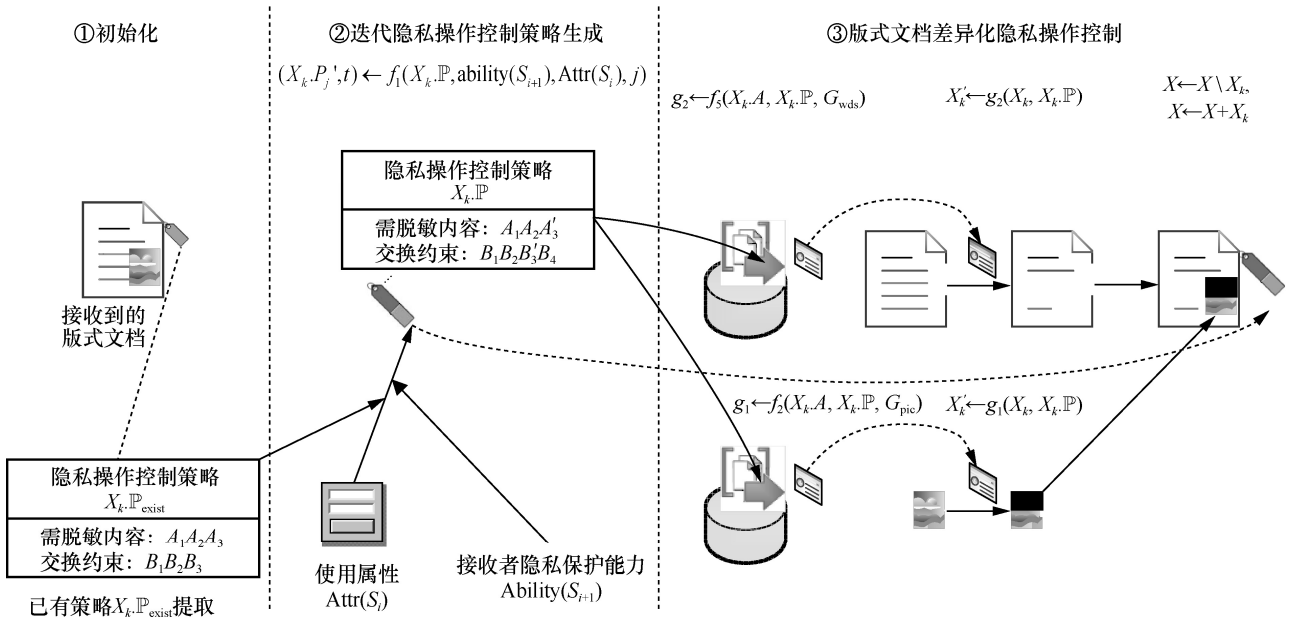

图 3　面向版式文档的细粒度隐私操作控制方法流程

权限。

2.2.2　迭代隐私操作控制策略生成

迭代隐私操作控制策略生成中，当前分享者 S_i 执行迭代隐私操作控制策略生成算法（算法 1），根据策略调整动作 t，动态迭代调整隐私操作控制策略 $X.\mathbb{P}$ 中的某条具体策略。版式文档 X 由 n 个信息分量组成，即 $X=\{X_1, X_2, \cdots, X_k, \cdots, X_n\}$，信息分量 X_k 定义为 $X_k=\langle c, A, \Gamma, \Omega, \Psi, \mathbb{P}\rangle$。

算法 1　迭代隐私操作控制策略生成算法

输入　版式文档 $X=\{X_1, X_2, \cdots, X_k, \cdots, X_n\}$，其中，每个信息分量 $X_k=\langle c, A, \Gamma, \Omega, \Psi, \mathbb{P}\rangle$，第 k 个信息分量的策略集合 $X_k.\mathbb{P}$，当前分享者 S_i，接收者 S_{i+1}

1) $n \leftarrow |X|$
2) for k in 1 : n do
3)　　$X_k.\mathbb{P} \leftarrow X_k$
4)　　$m \leftarrow |X_k.\mathbb{P}|$
5)　　for j in 1 : m do
6)　　$(X_k.P_j', t) \leftarrow f_1(X_k.\mathbb{P}, \text{ability}(S_{i+1}), \text{Attr}(S_i), j)$
7)　　　if $t = \text{DELETE}$ then
8)　　　　$X_k.\mathbb{P} \leftarrow X_k.\mathbb{P} \setminus X_k.P_j$
9)　　　elseif $t = \text{MODIFY}$ then
10)　　　　$X_k.\mathbb{P} \leftarrow X_k.\mathbb{P} \setminus X_k.P_j$
11)　　　　$X_k.\mathbb{P} \leftarrow X_k.\mathbb{P} + X_k.P_j'$
12)　　　elseif ⋯ then
13)　　　　⋯
14)　　　end if
15)　　　if ⋯ then
16)　　　　⋯
17)　　　end if
18)　　end for
19) end for

针对版式文档 X 中的 n 个信息分量遍历执行算法 1，从某一信息分量 X_k 中提取其隐私操作控制策略 $X_k.\mathbb{P}$（第 3)行），对隐私操作控制策略 $X_k.\mathbb{P}$ 中的每条策略逐一进行调整。

调用策略调整虚函数 f_1，得到策略调整动作 t 和修正后的策略 $X_k.P_j'$（第 6)行）。对于版式文档的某个信息分量 X_k，基于隐私操作控制策略 $X_k.\mathbb{P}$，结合当前分享者 S_i 使用属性 Attr(S_i)、接收者 S_{i+1} 的隐私保护能力 Ability(S_{i+1})等因素，对信息分量 X_k 的第 j 条隐私操作控制策略 $X_k.P_j$ 进行修正，得到调整后的策略 $X_k.P_j'$，逐条迭代生成隐私操作控制策略 $X_k.\mathbb{P}$。其中，f_1 是一个虚函数，读者可根据实际场景进行调整；f_1 参数中的 j 表示当前处理的第 j 条策略；$X_k.\mathbb{P}$ 作为 f_1 参数是考虑到调整 $X_k.P_j$ 的时候与其他策略存在冲突。防护能力是一个集合，本文不作具体的约束定义，在具体应用该集合的内容时可以根据对应的应用场景进行约束定义，例如，Ability.hardware 表示硬件防护能力。使用属性也是一个集合，本文也不作具体的约束定义，在具体应用该集合的内容时也可以根据对应的应用场景进行约束定义，例如，Attr.scene 表示场景，Attr.desire 表示操作要求等。

算法 1 的第 7)行～第 14)行根据 f_1 返回的策略调整动作 t，对传递的隐私操作控制策略进行调整。

当 t 为 DELETE 时，表示该条策略 $X_k.P_j$ 的内容已进行过隐私操作控制，后续不需再次进行该操作控制，即将该条策略 $X_k.P_j$ 从 $X_k.\mathbb{P}$ 中删除；若在当前分享者接收前该条策略对应的内容已经被交换边界控制进行了过滤处理，即该条策略 $X_k.P_j$ 作用的对象已不存在，则将该策略从 $X_k.\mathbb{P}$ 中删除（第 7)行和第 8)行）。例如，已有策略要求对所有姓“王”的姓名脱敏成“王**”，如果当前分享者接收到的文档中已将“王小二”脱敏成“王**”，此时当前分享者就可以删除这条策略；如果当前分享者发布的信息中已将“王小二”脱敏成“王**”，此时交换边界控制也不需要该条策略。

当 t 为 MODIFY 时，表示该条策略 $X_k.P_j$ 的内容已进行过部分的隐私操作控制，但需要再次进行更细粒度的控制，此时依据隐私操作控制策略 $X_k.\mathbb{P}$，结合使用属性，生成一个新的策略子集 $X_k.P_j'$ 来替换 $X_k.P_j$；若在当前分享者接收时就已经被交换边界控制进行了部分过滤，此时被过滤部分对应的策略可以作相应调整，即需生成一个新的策略子集 $X_k.P_j'$ 来替换 $X_k.P_j$（第 9)行～第 11)行）。例如，已有策略要求将“王小二”脱敏成“王小*”，当前分享者要求将所有姓“王”的姓名脱敏成“王**”，则需对该条策略 $X_k.P_j$ 进行调整；当前分享者在接收前，交换边界控制就已经将所有“姓 XY”的姓名过滤成“姓 X*”，当前分享者要求对“王小二”脱敏成“王**”，则此时需将该策略调整为对“王小*”脱敏成“王**”。

考虑到策略调整的多样性，算法 1 预留了为其他策略调整动作的情况（用省略号表示），以供实际应用中的拓展（第 12)行～第 14)行）。例如，当 t 为 REMAIN 时，表示当前策略 $X_k.P_j$ 执行内容未曾出现在隐私操作控制策略 $X_k.\mathbb{P}$ 中，此时不对 $X_k.\mathbb{P}$ 进行任何操作。例如，已有策略中要求对所有姓“王”的姓名脱敏成“王**”，当前分享者要求对所有姓“赵”的姓名脱敏成“赵**”，则在 $X_k.\mathbb{P}$ 中保留该条策略。

考虑到策略处理的多样性，算法 1 的第 15)行～第 17)行根据实际应用场景存在其他的策略调整、修改等处理方式（用省略号表示），可参照第 7)行～第 14)行进行类似处理。在执行完所有策略调整操作后，得到最终隐私操作控制策略。

2.2.3 版式文档差异化隐私操作控制

版式文档差异化隐私操作控制中，对于版式文档 X，基于迭代生成的隐私操作控制策略 $X.\mathbb{P}$，利用不同信息分量在不同模态下执行隐私操作控制算法（算法 2），对信息分量 X_k 进行差异化脱敏操作控制、交换边界控制和本地使用控制等。

算法 2 版式文档差异化隐私操作控制算法

输入 版式文档 $X=\{X_1, X_2, \cdots, X_k, \cdots, X_n\}$，其中，每个信息分量 $X_k=\langle c, A, \Gamma, \Omega, \Psi, \mathbb{P}\rangle$，图片脱敏算法库 G_{pic}，文字脱敏算法库 G_{wds}，分享者 S_i，接收者 S_{i+1}，操作控制目的 para.opt

1) $n \leftarrow |X|$
2) for k in 0 : n do
3) switch $X_k.c$.type do
4) case PICTURE do
5) if (para.opt.dataMasking = true) then
6) $g_1 \leftarrow f_2(X_k.A, X_k.\mathbb{P}, G_{\text{pic}})$
7) $X_k' \leftarrow g_1(X_k, X_k.\mathbb{P})$
8) $X \leftarrow X \setminus X_k$
9) $X \leftarrow X + X_k'$
10) end if
11) if (para.opt.broadControl = true) then
12) $\text{OP}_{\text{bc}} \leftarrow f_3(X_k, \text{para.opt.direction}, X_k.\mathbb{P})$
13) execute OP_{bc}
14) end if
15) if (para.opt.localControl = true) then
16) $\text{OP}_{\text{lc}} \leftarrow f_4(X_k, \text{para.opt.mod}, S_i, S_{i+1}, X_k.\mathbb{P})$
17) execute OP_{lc}
18) end if
19) if … then
20) …
21) end if
22) case WORDS do
23) if (para.opt.dataMasking = true) then
24) $g_2 \leftarrow f_5(X_k.A, X_k.P, G_{\text{wds}})$
25) $X_k' \leftarrow g_2(X_k, X_k.\mathbb{P})$
26) $X \leftarrow X \setminus X_k$
27) $X \leftarrow X + X_k'$
28) end if
29) if (para.opt.broadControl = true) then
30) $\text{OP}_{\text{bc}} \leftarrow f_6(X_k, \text{para.opt.direction}, X_k.\mathbb{P})$
31) execute OP_{bc}
32) end if
33) if (para.opt.localControl = true) then
34) $\text{OP}_{\text{lc}} \leftarrow f_7(X_k, \text{para.opt.mod}, S_i, S_{i+1}, X_k.\mathbb{P})$
35) execute OP_{lc}
36) end if
37) if … then
38) …
39) end if
40) case … do
41) …
42) end switch
43) end for

算法 2 是对隐私操作控制过程的抽象，对于版式文档的某个信息分量 X_k，基于隐私操作控制策略 $X_k.\mathbb{P}$ 根据当前信息分量内容 $X_k.c$ 的模态，结合具体操作场景，对信息分量 X_k 进行具体的差异化脱敏操作控制、交换边界控制和本地使用控制 3 种典型的操作控制模式，具体如下。

1) 差异化脱敏操作控制

差异化脱敏操作控制是依据算法 1 迭代生成的隐私操作控制策略 $X_k.\mathbb{P}$，综合考虑信息分量 X_k 的隐私属性向量 $X_k.A$ 和图片脱敏算法库 G_{pic} 等因素，选择一个脱敏算法 g_1（第 5)行～第 10)行），对信息分量 X_k 进行差异化脱敏。

图片脱敏算法的选择抽象化为虚函数f_2(第6)行)，该函数有 3 个参数，分别为信息分量 X_k 的隐私属性向量 $X_k.A$，表示该信息分量所需的基本保护程度；信息分量 X_k 的隐私操作控制策略 $X_k.\mathbb{P}$，包含所有分享者对脱敏操作控制的要求；图片脱敏算法库 G_{pic}，表示可备选脱敏算法，G_{pic} 面向多种图片格式且适应多种版式文档底层格式，可以对图片本身进行脱敏，并不是简单的图层覆盖。

图片脱敏算法选择虚函数f_2可根据实际应用场景进行约束定义，内部构造参数也可改变，以实现差异化的脱敏操作控制。该函数根据脱敏要求和不同算法的效果，实现对算法库 G_{pic} 中算法的统一管理和调配，确定使用当前应用场景对应的脱敏算法 g_1，具体如何选择适合对应场景的脱敏算法 g_1 不是本文的重点讨论内容。

2) 交换边界控制

交换边界控制是指依据隐私操作控制策略 $X_k.\mathbb{P}$ 和交换方向 para.opt.direction 等要素，在交换边界上对版式文档的某个信息分量 X_k 实施部分过滤、全部过滤和放行等控制操作（第 11)行～第 14)行）。

para.opt.direction 表示分享的交换方向，包括传入、传出等。限制传入的目的是严控信息非授权流入，不能将违背策略的内容进行添加。例如，即时通信系统内平台审核发布的文档，若文档中有违背策略的内容则自动过滤而不得发布。限制传出的目的是防止信息泄露，如跨域、跨网关、跨朋友圈等的分享，且提供文档溯源方法防止非授权分享行为的抵赖。

图片交换边界控制判断抽象化为虚函数 f_3（第 12)行），该参数可根据即时通信系统内和当前分享者 S_i 设定的交换边界控制规则调整设定，实现信息分量 X_k 是否需要进行交换边界控制及交换边界控制的程度等细粒度的操作控制。

判断结果 OP_{bc} 包括对图片的部分过滤、全部过滤和放行等行为。对于不同的判断结果，OP_{bc} 执行不同的操作控制。若判断结果 OP_{bc} 为全部过滤，则该图片内容不可转发分享；否则，仍可分享。

3) 本地使用控制

本地使用控制是在终端、后台服务器等设备上依据隐私控制策略 $X_k.\mathbb{P}$，综合考虑当前分享者 S_i、接收者 S_{i+1} 以及分享该文档的交换设备 para.opt.mod 等因素，使用图片本地使用控制虚函数 f_4 对信息分量 X_k 进行的操作，包括但不限于信息分量的显示、打印、复制、粘贴和转发等操作行为，算法 2 中将此部分功能的实现统一抽象为第 15)行～第 18)行。

图片本地使用控制虚函数 f_4 可根据当前分享者 S_i 设定的本地使用控制规则调整设定，相应参数可根据实际情况调整，实现根据申请查看该信息的人员、方式、位置、设备、时间等功能，以此判断该信息分量 X_k 是否需要进行本地使用控制及如何进行控制等。该函数的详细设置不是本文的重点讨论范畴，故不再赘述。

4) 隐私操作控制方式拓展

隐私操作控制不限于上述的差异化脱敏操作控制、交换边界控制和本地使用控制，还可支持其他隐私操作控制方式的拓展（第 19)行～第 21)行），可参照第 5)行～第 18)行进行类似处理。

对于版式文档的某个信息分量 X_k，依据当前内容 $X_k.c$，若所属模态为文字，与图片模态类似，先根据操作控制目的 para.opt 的不同，执行差异化脱敏操作控制、交换边界控制和本地使用控制中的一种或多种（第 22)行～第 39)行）。其中，对于文字的交换边界控制，判断结果 OP_{bc} 包括对信息分量的不修改、部分修改和彻底清空。只有当判断结果 OP_{bc} 不为彻底清空时，该信息分量 X_k 才可转发分享；否则，不可分享。

算法2还预留了其他可嵌入版式文档的模态处理情况(第 40)行～第 42)行)，具体实现可参照第 4)行～第 21)行进行类似处理。

2.2.4 隐私操作控制策略表述

由于本文方法采取两次加密机制，因此在执行隐私操作控制前，当前分享者 S_i 在接收到版式文档 X 时，先用自身的私钥将文档进行外层解密，得到内容仍为密文的文档和已有的隐私操作控制策略 $X.\mathbb{P}_{\text{exist}}$；再发送身份认证请求，通过认证后获得密钥解密文档内容，完成内层解密。

在执行隐私操作控制后，当前分享者 S_i 首先将隐私操作控制策略 $X.\mathbb{P}$ 嵌入文档中；然后告知允许的接收者 S_{i+1} 范围，并申请获得文档内容加密密钥，对文档进行内层加密，得到策略和内容加密后的文档；最后用接收者 S_{i+1} 的公钥对文档内容和策略进行整体加密，实现外层加密。

本文方法中版式文档是将隐私操作控制策略嵌入注释层，成为元数据的补充内容。本文方法对隐私

操作控制策略的结构化描述如图 4 和图 5 所示。

```
DESENSITIZE control-constraints cname
{ targetID , opuser , optime [, new_filename]
AS
{ performtype : ptypedetails }
}* hashsign;
```

图 4 脱敏操作控制策略实例

```
ASSIGN control-constraints cname
{ targetID , opuser , optime , globalsets ,
AS {
[{ rangelist : { < rangetype : rtypedetails , localsets > } }] [,]
[{ devicelist : { < devchoice : devdetails , localsets > } }] }
}* hashsign;
```

图 5 交换边界控制和本地使用控制策略实例

脱敏操作控制策略实例如图 4 所示。其含义为：按照名为 cname 的隐私操作控制策略内容执行脱敏操作控制（该句的校验值为 hashsign），执行对象参照 performtype 中选择的内容及其细则 ptypedetails（例如指定关键字/词、正则特定内容或指定图片等）。其中，targetID 表示执行该策略约束的文档 ID；opuser 表示设置该策略的操作者；optime 表示设置该策略的时间；new_filename 表示脱敏后新生成文档的名字，该内容为选填，可由分享者设置策略时填写，若分享者未填写，则脱敏后文档名由系统自动填写；performtype 表示执行脱敏操作控制的类型，可选的某个关键字/词、正则特定内容、指定图片，即 performtype:= keywords|regular|pictures ； ptypedetails 表示对 performtype 不同类型的细节设定。

交换边界控制和本地使用控制策略实例如图 5 所示。其含义为句式统一开头与脱敏操作控制策略相同，新增的 globalsets 表示对该策略设置的整体要求是全局（global）还是策略单项自定义（individual）。1)对于交换边界控制，当 rangelist 为内网 LANIP 或外网 WANIP 时，rtypedetails 就可以包括全局网络“*”、详细的单个 IP 地址或带有“X”的 IP 网段。其中，localsets 表示针对某一方面策略的要求，也是可选的（可读、可写、可显示、可删除、可修改、可复制、可交换），即 localsets := read | non-read | write | non-write | display | non-display | delete | non-delete | modify | non-modify | copy | non-copy | communicable | non-communicable。2)对于本地使用控制，①对于指定设备进行操作控制，devchoice 表示设备指定方式的判断，可以是对设备类型 devtype 进行约束，也可以是对指定设备机器码 devspecial 进行约束，即 devchoice := devtype | devspecial，devtype 表示设备类型，可选的有手机、平板电脑等，即 devtype := phone | pad，devspecial 表示指定某台设备（指定机器码）；②对于指定人员进行操作控制，当 rangetype 为 rangeuser 时，此时 rtypedetails 表示指定人员名单。

2.3 攻击模型与安全性分析

本文重点关注设计并实现即时通信系统内的版式文档的隐私操作控制。针对不同隐私操作控制策略，在面向不同版式文档时，本文方法中涉及的脱敏算法的选择相互独立。为实现版式文档的隐私操作控制，本文方法攻击者的攻击方式归纳为被动攻击者和主动攻击者。

被动攻击者是指集成了身份验证功能的普通社交网络服务器。假设这样的服务器是诚实但好奇的（HBC, honest-but-curious），既支持版式文档的交换，又管控身份认证功能，从而进行监测和查看，获取版式文档和其中嵌入的隐私操作控制策略。主动攻击者是指某一个能够接收版式文档的分享者，通过剥离、伪造、篡改隐私操作控制策略，或者借助得到的权限非法扩充自身权限。

为保障版式文档隐私操作控制过程中的完整性和安全性，本文利用基于公钥基础设施（PKI, public key infrastructure）的身份验证和双层加密机制，可保证版式文档在交换控制过程中的安全，同时利用身份验证机制可保证隐私操作控制策略的不可否认性。由于 PKI 技术是成熟的技术，本文将不再对该安全问题进行详细的证明。

根据所设定的攻击模型，第一种攻击者是 HBC 服务器这样的被动攻击者，主要有 3 种攻击情况：①服务器收集原始未脱敏和每次分享时脱敏的版式文档；②服务器收集每次分享时版式文档中的隐私操作控制策略；③服务器收集所有脱敏算法及参数。

面对第①种情况，根据法律条款规定是不得将个人聊天记录和版式文档直接交换的，故暂不考虑其安全性问题。

面对第②种情况，利用加密技术对隐私操作控制策略进行加密，可以抵御服务器获得隐私操作控

制策略 $\mathbb{P}$ 中的内容。

面对第③种情况，所有的脱敏算法均是针对版式文档本身的脱敏，由于脱敏算法具有不可逆性，信息一旦脱敏，即使攻击者知晓脱敏算法及其参数也不能还原出真实信息。

第二种攻击者是某一个分享版式文档的分享者，可作为主动攻击者。

首先，传播链上的某一分享者即使通过其他途径收到了自身本不可接收的版式文档，也只有使用私钥进行了外层解密，提取到了已有隐私操作控制策略 $X.\mathbb{P}_{\text{exist}}$ 并通过了身份认证，且成功进行了内层解密的文档的分享者，才可查看该文档内容；如果其利用暴力破解方式，将隐私操作控制策略与信息通过剥离、修改等方式绕开双层加密机制中的任意环节，则会参考数字版权技术的方法，启动自毁程序，将版式文档销毁。

由于隐私操作控制策略在追加时必须通过语义检验机制，当作为攻击者的分享者 S_i 赋予接收者超过自己可赋予的更高权限时，则会出现语义检验不通过，无法追加、执行该条隐私操作控制策略的情况。

将算法 1 中的策略调整虚函数 f_1 的参数进行抽象，对于当前分享者 S_i 而言，依据接收到来自上一分享者 S_{i-1} 的隐私操作控制策略 $X.\mathbb{P}_{i-1}$，再结合当前分享者 S_i 设置使用属性 Attr(S_i)和以接收者隐私保护能力 Ability(S_{i+1})为核心等因素，生成当前分享者 S_i 的隐私操作控制策略 $X.\mathbb{P}_i$

$$X.\mathbb{P}_i = F\left(X.\mathbb{P}_{i-1}, \text{Attr}(S_i), \text{Ability}(S_{i+1}), f(S_i, S_{i+1})\right)$$

其中，$f(S_i, S_{i+1})$表示当前分享者 S_i 及接收者 S_{i+1} 的隐私操作控制相关要求。特别地，当 i=1 时，分享者 S_1 的隐私操作控制策略为

$$X.\mathbb{P}_1 = F\left(\text{Attr}(S_1),\ \text{Ability}(S_{i+1}), f(S_1, S_2)\right)$$

在版式文档交换过程中，需保证隐私操作控制策略逐渐严格，即传播链上后续的分享者不能获得比先前分享者更多的权限。系统会对每一条新加入的策略进行校验，且每条策略都需符合

$$X.\mathbb{P}_i \subseteq \left(X.\mathbb{P}_{i-1} \cup \text{Attr}(S_i) \cup \text{Ability}(S_{i+1}) \cup f(S_i, S_{i+1})\right) \subseteq X.\mathbb{P}_{i-1}$$

假设第 i、i+1 和 i+2 个分享者为 S_i、S_{i+1} 和 S_{i+2}，则对应的第 i、i+1 和 i+2 个分享者的隐私操作控制策略分别为 $X.\mathbb{P}_i$、$X.\mathbb{P}_{i+1}$ 和 $X.\mathbb{P}_{i+2}$，则有

$$X.\mathbb{P}_{i+2} \subseteq \left(X.\mathbb{P}_{i+1} \cup \text{Attr}(S_{i+2}) \cup \text{Ability}(S_{i+3}) \cup f(S_{i+2}, S_{i+3})\right) \subseteq X.\mathbb{P}_{i+1} \subseteq \left(X.\mathbb{P}_i \cup \text{Attr}(S_{i+1}) \cup \text{Ability}(S_{i+2}) \cup f(S_{i+1}, S_{i+2})\right) \subseteq X.\mathbb{P}_i$$

若作为攻击者的分享者 S_i 想要获取更多的权限，与接收者 S_{i+1} 以及下一个接收者 S_{i+2} 进行合谋，获取更多权限。但是由于

$$X.\mathbb{P}_{i+2} \subseteq X.\mathbb{P}_{i+1} \subseteq X.\mathbb{P}_i \subseteq X.\mathbb{P}_{i-1}$$

分享者 S_i 的所有隐私操作控制策略 $X.\mathbb{P}_i$ 为分享者 S_i 分享版式文档过程中的隐私操作控制约束。令 Prv_i 表示第 i 个分享者 S_i 可获得的权限，则对于分享者 S_i、S_{i+1} 和 S_{i+2}，有

$$\text{Prv}_{i+2} \subseteq \text{Prv}_{i+1} \subseteq \text{Prv}_i \subseteq \text{Prv}_{i-1}$$

即 Prv_{i+2} 是 Prv_{i+1} 的子集，Prv_{i+1} 是 Prv_i 的子集，故作为攻击者的分享者 S_i 无法获取超过自身所拥有的更多权限。

3　实验及分析

为验证本文方法，本节研发了 OFD [22]的隐私操作控制前后台原型系统，包括 Android 客户端 APP 和后台服务器。客户端 APP 基于数科网维提供的 API 进行研发，负责版式文档信息的接收，已有隐私操作控制策略的提取，隐私操作控制策略的迭代生成、执行和安全传递等功能；后台服务器负责客户端用户的身份认证功能。本节开发的 Android 客户端 APP 已在 GitHub 上发布，具体所支持的脱敏算法如表 2 所示。

表 2　　当前系统支持的脱敏算法

算法库	包含的脱敏算法
文字 G_{wds}	空白置换算法
	特殊符号置换算法
	指定文字置换算法
	假名置乱算法
	部分置乱算法
图片 G_{pic}	全黑遮蔽算法
	全透明置换算法

3.1 实验环境

本文实验使用多台 Android 手机（6 GB RAM，Android 9 系统）和平板电脑（6+2 GB RAM，Android 12 系统）作为客户端设备，使用一台服务器（2 GB RAM，单核，CentOS 7+Mysql 5.7.37 环境）作为后台管理服务器（测试设备不限于上述规格要求）。基于该实验环境，测试基于朋友圈分享 OFD 过程中的隐私操作控制效果（为保护测试人员的个人隐私信息，本文用李小一、李小二、李小三、王小一、王小二、赵小一、赵小二、赵小三和赵小四等代替真实姓名）。

3.2 实验过程与结果分析

李小一等人基于个人朋友圈对版式文档 X 的交换过程如图 6 所示，①、②、③代表三轮交换过程。其中所涉及的控制策略描述方法不是本文的主要贡献，不进行详细赘述。详细的实验过程如下。

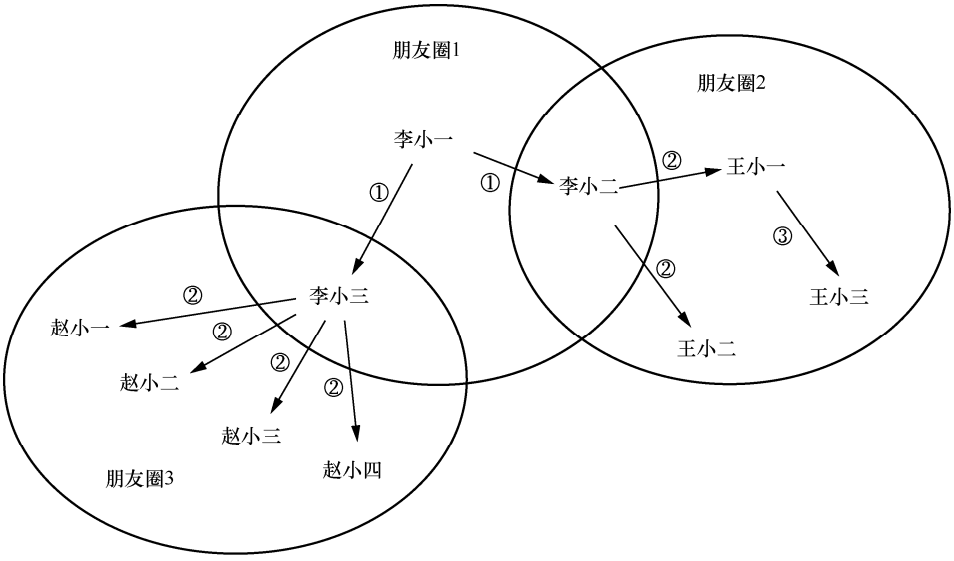

图 6 李小一等人基于个人朋友圈对版式文档 X 的交换过程

1) 同一文档图片的差异化脱敏控制

为验证同一文档图片的差异化脱敏控制功能，实验中文档持有者李小一（首次分享者）根据自身隐私保护需求，对分享的版式文档 X（intro.ofd）设置隐私操作控制策略：向李小二发送的文档中第一张图片做全黑遮蔽处理，向李小三发送的文档不做处理。控制策略以注释的方式嵌入版式文档中，示例性的控制策略如图 7 所示；策略正确执行后的效果如图 8 所示，图 8(a)表示李小二接收到文档的第一张图片被全黑遮蔽，其余内容正常显示，图 8(b)表示李小三接收到文档的所有图文信息均可以正常显示。

```
DESENSITIZE control-constraints cc_share_ofdfile
{ targetID : 29665 ,
opuser : LiXiaoYi ,
optime : 2023-01-27:10:45:35 ,
newfile :intro.ofd ,
AS {
pictures : < { 1 }
}
} hashsign;
```

图 7 分享者李小一设置的同一图片的差异化脱敏控制策略

(a) 李小二的图片遮蔽效果 (b) 李小三的图文正常显示效果

图 8 分享者李小一策略正确执行后的效果

2) 文本信息细粒度差异化脱敏控制

为验证文本信息细粒度差异化脱敏控制功能，实验中李小二通过朋友圈 2 再次将文档分享给好友王小一和王小二，并根据自身隐私保护需求，在已有的隐私操作控制策略基础上设置新的控制策略：向王小一发送的文档中，对选中的字段姓名“李小

一”进行细粒度脱敏，对选中的身份证号码后 6 位“015222”进行脱敏；向王小二发送的文档中，对选中的完整身份证号码进行全部脱敏，数字全部脱敏为“*”，对姓名字段不做约束。控制策略以批注的方式嵌入版式文档，示例性的控制策略如图 9 所示；策略正确执行后的效果如图 10 所示，图 10(a)表示王小一接收到的文档，姓名字段已脱敏为“***”，身份证号码字段已脱敏为“370683199911******”，图 10(b)表示王小二接收到的文档，姓名字段可见，身份证号码字段已全部脱敏为“**********”。

```
toWangXiaoYi:
Anoots Boundary : "32.0088 114.0885 16.6943 5.1429";
Anoots Boundary : "79.2135 235.3521 12.6575 2.9083";
ASSIGN control-constraints cname
{
 targetID : 29666 ,
 opuser : LiXiaoEr ,
 optime : 2023-01-27:22:02:10 ,
 globalsets : { individual } ,
AS {
 rangelist : { < rangeuser : { WangXiaoYi } ,
 localsets : { non-display } > }
} hashsign;

toWangXiaoEr:
Anoots Boundary : "51.9343 235.3521 39.9367 2.9083";
ASSIGN control-constraints cname
{
 targetID : 29667 ,
 opuser : LiXiaoEr ,
 optime : 2023-01-27:22:09:22 ,
 globalsets : { individual } ,
AS {
 rangelist : { < rangeuser : { WangXiaoEr } ,
 localsets : { non-display } > }
} hashsign;
```

图 9　分享者李小二设置的细粒度差异化脱敏控制策略

（a）王小一的脱敏控制效果　　（b）王小二的脱敏控制效果

图 10　分享者李小二策略正确执行后的效果

3) 二次分享的迭代脱敏控制

为验证文本信息二次分享的迭代脱敏控制功能，实验中王小一通过朋友圈 2 再次将文档分享给好友王小三，并根据自身隐私保护需求，在已有的隐私操作控制策略基础上设置新的控制策略：对身份证号码剩余的 12 位进行迭代脱敏控制。控制策略以批注的方式嵌入版式文档，示例性的控制策略如图 11 所示。策略正确执行后的效果如图 12 所示，即王小三接收到的文档，身份证号字段已全部迭代脱敏为“**********”。

```
Anoots Boundary : "32.0088 114.0885 16.6943 5.1429";
Anoots Boundary : "51.9343 235.3521 39.9367 2.9083";
ASSIGN control-constraints cname
{
 targetID : 29668 ,
 opuser :WangXiaoYi,
 optime : 2023-01-27:22:02:19 ,
 globalsets : { individual } ,
AS {
 rangelist : { < rangeuser : { WangXiaoSan } ,
 localsets : { non-display } > }
} hashsign;
```

图 11　分享者王小一设置的迭代脱敏控制策略

图 12　王小三的迭代脱敏控制效果

4) 细粒度交换边界控制

为验证交换边界控制功能，实验中李小三通过朋友圈 3 向好友赵小一和赵小二再次分享文档，并根据自身隐私保护需求，在已有的隐私操作控制策略基础上迭代设置新的控制策略：李小三希望自己所在位置 500 m 范围外的好友无法查看文档的手机号码，1 km 范围外的好友无法查看文档的邮箱。控制策略以批注的方式嵌入版式文档，示例性的控制策略如图 13 所示；策略正确执行后的效果如图 14 所示，图 14(a)表示赵小一在李小三所在位

置 500 m 以内，能正常查看该文档中的手机号码和邮箱，图 14(b)表示赵小二在李小三所在位置 500 m 以外、1 km 以内，能正常查看该文档中的邮箱，但不能查看手机号码。

```
toZhaoXiaoYi:
Anoots Boundary : "54.2839 214.4395 23.3973 2.9083";
Anoots Boundary : "45.1357 256.2394 41.4689 3.4713";
ASSIGN control-constraints cname
{ targetID : 29669 ,
  opuser : LiXiaoSan ,
  optime : 2023-01-27:22:17:13 ,
  globalsets : { individual } ,
AS {
  loclist : { < gps : { lon : 116.293631 ,
  lat : 40.019484 , rad : 0.5 } ,
  localsets : { display } > }
} hashsign;

toZhaoXiaoEr:
Anoots Boundary : "45.1357 256.2394 41.4689 3.4713";
ASSIGN control-constraints cname
{
  targetID : 29670 ,
  opuser : LiXiaoSan ,
  optime : 2023-01-27:22:17:16 ,
  globalsets : { individual } ,
AS {
  loclist : { < gps : { lon : 116.293631 ,
  lat : 40.019484 , rad : 1 } ,
  localsets : { display } > }
} hashsign;
Anoots Boundary : "54.2839 214.4395 23.3973 2.9083";
ASSIGN control-constraints cname
{
  targetID : 29671 ,
  opuser : LiXiaoSan ,
  optime : 2023-01-27:22:19:32 ,
  globalsets : { individual } ,
AS {
  loclist : { < gps : { lon : 116.293631 ,
  lat : 40.019484 , rad : 0.5 } ,
  localsets : { display } > }
} hashsign;
```

图 13　分享者李小三设置的细粒度交换边界控制策略

（a）赵小一的交换控制效果　（b）赵小二的交换控制效果

图 14　分享者李小三细粒度交换边界控制策略正确执行后的效果

5) 本地使用控制

为验证本地使用控制功能，实验中李小三向自己的好友赵小三和赵小四分享该文档，并根据自身隐私保护需求，设置设备机器码约束控制：文档只能在机器码为“8653200042806071”的设备上正常打开并可以查看文档中的电话号码字段，除此机器码约束之外的设备正常打开文档后，电话号码字段的内容不显示。设置策略以批注的方式嵌入版式文档，示例性的控制策略如图 15 所示；策略正确执行后的效果如图 16 所示，图 16(a)表示赵小三的设备机器码与本地使用控制策略中的约束条件保持一致，可以正常打开该文档并查看电话号码，图 16(b)表示赵小四的机器码不在策略约束的范围内，能正常打开该文档但文档中的电话号码字段的内容不显示。

```
Anoots Boundary : " 47.4979 245.7662 14.8757 2.9083";
ASSIGN control-constraints cname
{
  targetID : 29672 ,
  opuser : LiXiaoSan ,
  optime : 2023-01-27.22.22.09 ,
  globalsets : { individual } ,
AS {
  devicelist : { < devspecial : 8653200042806071 ,
  localsets : { display } }
} hashsign;
```

图 15　分享者李小三的本地使用控制策略

（a）赵小三的本地控制效果　（b）赵小四的本地控制效果

图 16　分享者李小三本地使用控制策略正确执行后的效果

3.3　性能评估

本节实验主要评估隐私操作控制策略的生成、解析和执行等环节所增加的时间消耗，实验结果如表 3 和表 4 所示。实验中每个环节重复 10 次，将新增时间的平均值作为本次实验的时间消耗。

表 3　　首次隐私操作控制环节的时间消耗

脱敏模态	寻找信息分量的方式	策略生成/ms	策略解析/ms	策略执行/ms	策略生成和策略解析时间占比	策略执行时间占比
图片		7.00	2.00	83.00	9.78%	90.22%
文字	正则特定内容	7.00	1.00	226.00	3.42%	96.58%
	关键词	10.00	2.00	195.00	5.80%	94.20%
平均		8.00	1.67	168.00	5.44%	94.56%

表 4　　迭代隐私操作控制环节的时间消耗

首次脱敏信息分量模态及寻找信息分量的方式	迭代脱敏信息分量模态及寻找信息分量的方式	策略生成/ms	策略解析/ms	策略执行/ms	策略生成和策略解析时间占比	策略执行时间占比
图片	图片	6.00	1.00	76.00	8.43%	91.57%
	文字–正则特定内容	9.00	2.00	261.00	4.04%	95.96%
	文字–关键词	7.00	2.00	181.00	4.74%	95.26%
	平均	7.33	1.67	172.67	4.95%	95.05%
文字–正则特定内容	图片	9.00	3.00	76.00	13.64%	86.36%
	文字–正则特定内容	10.00	1.00	280.00	3.78%	96.22%
	文字–关键词	8.00	2.00	187.00	5.08%	94.92%
	平均	9.00	2.00	181.00	5.73%	94.27%
文字–关键词	图片	8.00	2.00	81.00	10.99%	89.01%
	文字–正则特定内容	8.00	1.00	264.00	3.30%	96.70%
	文字–关键词	9.00	2.00	177.00	5.85%	94.15%
	平均	8.33	1.67	174.00	5.43%	94.57%
平均		8.22	1.78	175.89	5.38%	94.62%

由表 3 和表 4 可知，不论是首次还是迭代隐私操作控制，不同信息分量的策略生成、策略解析和策略执行等平均时间消耗不高于 8.30 ms、1.80 ms 和 176.00 ms。

表 5 从延伸控制、迭代延伸控制、脱敏、迭代脱敏、交换边界控制、前端操作控制、后台操作控制、细粒度差异化保护等方面将本文方法与传统脱敏方法[23-28]进行对比。对比结果表明，本文方法在上述几个方面中明显优于传统脱敏方法。

4　结束语

本文针对隐私信息在即时通信系统内频繁共享等特点，提出了一个面向版式文档的细粒度隐私操作控制方法。该方法约束分享者对传播链上后续分享者的隐私操作控制。首先，提取信息中已携带的隐私操作控制策略和当前分享者的使用属性；其次，融合已有隐私操作控制策略，生成迭代隐私操作控制策略；最后，根据隐私操作控制策略，对版

表 5　　本文方法与传统脱敏方法对比

保护方法	延伸控制	迭代延伸控制	脱敏	迭代脱敏	交换边界控制	前端操作控制	后台操作控制	细粒度差异化保护
本文方法	√	√	√	√	√	√	√	√
基于匿名的脱敏方法	×	×	√	×	×	×	×	×
基于差分的脱敏方法	×	×	√	×	×	×	部分支持	×
基于信息论的脱敏方法	×	×	√	×	×	×	×	×

式文档进行隐私操作控制，包括但不限于细粒度差异化脱敏操作控制、交换边界控制和本地使用控制。为了验证方法的可行性和有效性，本文开发了一个针对 OFD 的隐私操作控制前后台原型系统，模拟基于朋友圈信息交换过程中的隐私操作控制效果，用户手动设置隐私操作控制要求，并对版式文档进行细粒度差异化隐私操作控制，在一组真实的实验数据上进行测试，实验结果证明了所提方法的有效性和效率。

未来工作中，在初始化阶段，版式文档中信息分量的自动生成会提升本文方法的自动化程度；在版式文档差异化隐私操作控制阶段，对于文档的差异化脱敏操作控制部分，引入隐私保护效果评估机制，以便更好地选出适合不同信息分量的脱敏算法，提高本文方法的有效性和效率；引入对接收者防护能力 Ability(S_{i+1})的实时评估机制，并将该结果与服务器所维护的用户数据库进行关联，以供当前分享者获取。

参考文献：

[1] FRAGKOS G, JOHNSON J, TSIROPOULOU E E. Dynamic role-based access control policy for smart grid applications: an offline deep reinforcement learning approach[J]. IEEE Transactions on Human-Machine Systems, 2022, 52(4): 761-773.

[2] ZHANG Q K, ZHU L, ZHAO K Y, et al. Dynamic permission access control model based on privacy protection[J]. Telecommunication Systems, 2022, 81(2): 191-205.

[3] LIN H, KAUR K, WANG X D, et al. Privacy-aware access control in IoT-enabled healthcare: a federated deep learning approach[J]. IEEE Internet of Things Journal, 2023, 10(4): 2893-2902.

[4] SANTOS D R D, MARINHO R, SCHMITT G R, et al. A framework and risk assessment approaches for risk-based access control in the cloud[J]. Journal of Network and Computer Applications, 2016, 74: 86-97.

[5] SANTOS D R D, WESTPHALL C M, WESTPHALL C B. A dynamic risk-based access control architecture for cloud computing[C]//Proceedings of 2014 IEEE Network Operations and Management Symposium (NOMS). Piscataway: IEEE Press, 2014: 1-9.

[6] NING J T, CAO Z F, DONG X L, et al. Auditable σ time outsourced attribute-based encryption for access control in cloud computing[J]. IEEE Transactions on Information Forensics and Security, 2018, 13(1): 94-105.

[7] YAN Z, LI X Y, WANG M J, et al. Flexible data access control based on trust and reputation in cloud computing[J]. IEEE Transactions on Cloud Computing, 2017, 5(3): 485-498.

[8] KARJOTH G, SCHUNTER M, WAIDNER M. Platform for enterprise privacy practices: privacy-enabled management of customer data[C]//Privacy Enhancing Technologies Symposium. Berlin: Springer, 2003: 69-84.

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

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

[11] NIU B, LI Q H, WANG H Y, et al. A framework for personalized location privacy[J]. IEEE Transactions on Mobile Computing, 2022, 21(9): 3071-3083.

[12] CHEN K K, LIU L. Privacy preserving data classification with rotation perturbation[C]//Proceedings of Fifth IEEE International Conference on Data Mining (ICDM'05). Piscataway: IEEE Press, 2005: 589-592.

[13] WANG L, NEAR J P, SOMANI N, et al. Data capsule: a new paradigm for automatic compliance with data privacy regulations[C]//Heterogeneous Data Management, Polyestrous, and Analytics for Healthcare. Berlin: Springer, 2019: 3-23.

[14] WANG L, KHAN U, NEAR J, et al. PrivGuard: privacy regulation compliance made easier[C]//2022 USENIX Security Symposium (USENIX Security). Berkeley: USENIX Association, 2022: 3753-3770.

[15] 李凤华, 李晖, 牛犇. 隐私计算理论与技术[M]. 北京: 人民邮电出版社, 2021.
LI F H, LI H, NIU B. Privacy computing theory and technology[M]. Beijing: Posts & Telecom Press, 2021.

[16] 李凤华, 孙哲, 吕梦凡, 等. 社交照片隐私保护机制研究进展[J]. 信息安全学报, 2018, 3(2): 41-61.
LI F H, SUN Z, LYU M F, et al. Research progress of photo privacy-preserving mechanisms in online social network[J]. Journal of Cyber Security, 2018, 3(2): 41-61.

[17] 李凤华, 孙哲, 牛犇, 等. 跨社交网络的隐私图片分享框架[J]. 通信学报, 2019, 40(7): 1-13.
LI F H, SUN Z, NIU B, et al. Privacy-preserving photo sharing framework cross different social network[J]. Journal on Communications, 2019, 40(7): 1-13.

[18] LI F H, SUN Z, NIU B, et al. An extended control framework for privacy-preserving photo sharing across different social networks[C]//Proceedings of 2019 International Conference on Computing, Networking and Communications (ICNC). Piscataway: IEEE Press, 2019: 390-394.

[19] LI F H, SUN Z, LI A, et al. HideMe: privacy-preserving photo sharing on social networks[C]//Proceedings of IEEE Conference on Computer Communications. Piscataway: IEEE Press, 2019: 154-162.

[20] 李凤华, 王彦超, 殷丽华, 等. 面向网络空间的访问控制模型[J]. 通信学报, 2016, 37(5): 9-20.
LI F H, WANG Y C, YIN L H, et al. Novel cyberspace-oriented access control model[J]. Journal on Communications, 2016, 37(5): 9-20.

[21] LI F H, LI H, NIU B, et al. Privacy computing: concept, computing framework, and future development trends[J]. Engineering, 2019, 5(6): 1179-1192.

[22] 电子文件存储与交换格式: LD/T 50.5-2016[S]. GB/T 33190-2016, 2016.
Electronic files storage and exchanges formats—fixed layout documents[S]. GB/T 33190-2016, 2016.

[23] SWEENEY L. K-anonymity: a model for protecting privacy[J]. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 2002, 10(5): 557-570.

[24] MACHANAVAJJHALA A, GEHRKE J, KIFER D, et al. L-diversity: privacy beyond k-anonymity[C]//Proceedings of 22nd International

Conference on Data Engineering (ICDE'06). Piscataway: IEEE Press, 2006: 24.

[25] DWORK C. Differential privacy: a survey of results[C]//International Conference on Theory and Applications of Models of Computation. Berlin: Springer, 2008: 1-19.

[26] MCSHERRY F, TALWAR K. Mechanism design via differential privacy[C]//Proceedings of 48th Annual IEEE Symposium on Foundations of Computer Science (FOCS'07). Piscataway: IEEE Press, 2007: 94-103.

[27] WU G Q, XIA X Y, HE Y P. Extending differential privacy for treating dependent records via information theory[J]. arXiv Preprint, arXiv: 1703.07474, 2017.

[28] 彭长根, 丁红发, 朱义杰, 等. 隐私保护的信息熵模型及其度量方法[J]. 软件学报, 2016, 27(8): 1891-1903.
PENG C G, DING H F, ZHU Y J, et al. Information entropy models and privacy metrics methods for privacy protection[J]. Journal of Software, 2016, 27(8): 1891-1903.

[作者简介]

尹沛捷（1995− ），女，陕西汉中人，中国科学院信息工程研究所博士生，主要研究方向为隐私计算、隐私保护。

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。

牛犇（1984− ），男，陕西西安人，博士，中国科学院信息工程研究所研究员、博士生导师，主要研究方向为数据安全、隐私计算。

罗海洋（1997− ），男，湖南娄底人，中国科学院信息工程研究所博士生，主要研究方向为隐私计算、隐私保护。

邝彬（2000− ），男，湖南永州人，中国科学院信息工程研究所博士生，主要研究方向为隐私计算、隐私保护。

张玲翠（1986− ），女，河北故城人，博士，中国科学院信息工程研究所高级工程师、硕士生导师，主要研究方向为网络与系统安全、数据安全。