基于双线性映射的图像编辑授权与举证

陈海霞[1] 黄欣沂[2] 张福泰[2] 宁建廷[2),3)] 宋永成[4]

[1)](福建师范大学数学与统计学院 福州 350000)

[2)](福建师范大学计算机与网络空间安全学院福建省网络安全与密码技术重点实验室 福州 350000)

[3)](中国科学院信息工程研究所信息安全国家重点实验室 北京 100093)

[4)](密码科学技术国家重点实验室 北京 100878)

摘 要 为有效鉴别与检测图像编辑行为是否经过授权,文章提出了基于公钥密码技术的图像编辑授权与举证方案.方案允许图像版权人对需授权图像进行初始认证并生成编辑许可证书;图像编辑人借助许可证书编辑图像并生成证据,以举证其对图像的编辑行为确实经过了授权;图像接收方(验证人)通过版权人和编辑人提供的证据验证图像编辑的有效性与合法性.文中方案可为图像编辑授权行为提供便捷的检测方法,便于图像接受方在发布图像之前,对图像使用是否已获得授权进行检测,从技术上规避侵权纠纷.方案基于双线性映射而构造,验证高效并具有可证明安全性.实验数据表明,虽然方案在密钥生成时计算开销较大,但证据的计算和验证仍然是高效实用的.通过与现有方案对比,在实现编辑授权的情况下,计算开销增加小于 10%.基于公钥密码技术的图像认证方案设计有望成为除数字水印和感知哈希技术以外,又一服务于图像安全应用的新型通用设计,相关研究可为图像编辑授权应用提供有效解决方案.

关键词 图像编辑授权;编辑举证;数据认证;双线性映射;可证明安全性

中图法分类号 TP309 **DOI 号** 10.11897/SP.J.1016.2022.02348

Image Editing Authorization and Proof from Bilinear Pairings

CHEN Hai-Xia[1] HUANG Xin-Yi[2] ZHANG Fu-Tai[2] NING Jian-Ting[2),3)] SONG Yong-Cheng[4]

[1)](*School of Mathematics and Statistics, Fujian Normal University, Fuzhou* 350000)

[2)](*Fujian Provincial Key Lab of Network Security & Cryptography, School of Computer and Cyber Security, Fujian Normal University, Fuzhou* 350000)

[3)](*State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing* 100093)

[4)](*State Key Laboratory of Cryptology, Beijing* 100878)

Abstract Each image is associated with its copyright. An image's copyright is a type of property that gives its owner/creator the exclusive right to transmit, publish and use her work. Protected by public low, the copyright owner can define how an image can be used by signing a licensing agreement with users who wishes to use or edit the image for fee. However, it has been challenging work to detect if an image is edited by an authorized entity. Traditional methods, such as watermarks and perceptual hashes, can help detect if the image has been edited with permissible operations, but fail to verify the identity of its potential users. As a result, traditional methods cannot provide sufficient technical supports for editing authorization that is required by image copyright holders. In this paper, an authentication scheme constructed from public-key cryptographic primitives is proposed to provide efficient solution for image editing authorization. The proposed scheme allows an image owner/copyright-holder to specify editing rules and authenticate the original image technically. The authenticated image is transmitted to an image editor together with a certificate

收稿日期:2021-06-09;在线发布日期:2022-06-01.本课题得到国家自然科学基金(61902070,62032005,61972094,62172096)资助.**陈海霞**,博士,中国计算机学会(CCF)会员,主要研究领域为图像认证与信息安全.E-mail:tummy7882@hotmail.com.**黄欣沂**(通信作者),博士,教授,博士生导师,中国计算机学会(CCF)会员,主要研究领域为密码学与信息安全.E-mail:xyhuang@fjnu.edu.cn.**张福泰**,博士,教授,博士生导师,中国计算机学会(CCF)会员,主要研究领域为密码学与信息安全.**宁建廷**,博士,教授,主要研究领域为公钥密码学与信息安全.**宋永成**,博士,主要研究方向为编码密码学与信息安全.

associated with some licensing behaviors. The certificate is computed by the image copyright holder and send to an authorized editor together with the image. After receiving an authorized image and its certificate, the image editor can process the image according to the certificate and compute supplementary proof to prove that the editing operation(s) are permissible and authorized. To avoid copyright infringement, an image receiver/verifier can verify the legality of the image with both of the evidence provided by the image holder and the editor. The new design helps the image receiver to identify if an image has been used legally before publishing it to keep away from disputation of copyrights. The scheme is constructed from bilinear pairings and provably secure. The security of these schemes is rigorously proved in the framework of provable security in cryptology. Different from those traditional non-cryptographic image authentication schemes (watermarks and perceptual hashes), the security here is independent of the size of sample space or times of experiments, and just depends on the security of cryptographic primitives used in the constructions. Experiments show that the proposed scheme is efficient and practical. Though the computation of key generation is time-consuming, since the key generation scheme is run only once in the whole lifetime of the system, and it can be deployed offline, the efficiency of the scheme is still satisfying. Concretely, the time cost of proving is about 70 milliseconds for 400 hundred operations, and verification time is less than 20 milliseconds (far less the time of key generation). In addition, compared with the most relevant scheme, our scheme achieves authorization with slight loss of efficiency, perhaps less than 10%, but the proving and verification are still efficient. The new design provides a new framework for research on image authentication together with digital watermarking and perceptual hashing, and we believe it will further facilitate image applications where image authorization is desirable. Scheme in this paper can also provide effective solutions for image applications where outsourced image operations in cloud computing are required.

Keywords　image editing authorization; editing proof; data authentication; bilinear pairings; provable security

1　引　言

图像都具有版权，图像版权在被创建时自动分配给创作者. 创作者(或称版权人)可以决定如何使用和处理该图像. 图像版权是法定权利，被定义为“一个人对他或她的原创作品的复制、出版和使用的专属权利”[1]. 知识产权法规定，任何人未经版权人许可，不得盗窃、复制或出售其他人作品. 侵权行为一旦发生，被侵权人可以通过法律手段主张自己的权利并向侵权人追责.

虽然受法律条款约束，侵权行为还是屡见不鲜. 为规避纠纷，绝大部分出版社或媒体机构，在决定采纳和出版用户的投稿作品之前，都会与投稿人签署图片使用协议，要求用户承诺其所提交的图片是原创或经过授权的，且对图片的使用得到了版权人的许可.

图片使用协议是由图片版权人和被授权人共同签署的一组约束条款. 条款中，版权人规定被授权人在何种情况下使用图像、以及以何种方式编辑图像等. 然而，此类协议只是认定使用人是否侵权的依据，不具备鉴定能力，在实际使用过程中，协议常常需要与配合一定的技术方法，例如，数字水印、感知哈希等图像取证技术，以鉴定并检测图像编辑使用是否合法.

“数字水印”(Watermarking)的概念最早由 Tirkel 等人[2-3]在 1992 年提出，并在次年首次成功实现隐写频谱水印的嵌入和提取. 数字水印技术，尤其是鲁棒水印(Robust Watermarking)，是图像版权保护(Copyright Protection)的重要技术[4-5]. 该技术通过向图像中嵌入版权信息进行版权声明，当侵权行为发生时，通过提取图像中的水印信息进行举证，以追究侵权人的责任. 鲁棒水印具有隐藏性、稳健性等特征，对绝大部分图像操作不敏感. 鲁棒水印的稳健性

可以有效阻止侵权人对水印信息进行破坏或移除，以保护版权信息.经过长时间的研究，利用数字水印技术进行版权保护的研究已经取得了积极进展，产生了一些有意义的研究成果[6-8].鲁棒水印可以有效检测图像版权信息，追溯图像来源，但不考虑对图像编辑行为进行约束，从而不适用于图像编辑授权.

图像认证(Image Authentication)的目标是验证图像内容真实性和完整性[9]，该技术可以对试图改变图像内容的攻击行为进行检测，保障图像版权人的合法权益.图像认证主要有半脆弱水印(Semi-fragile Watermarking)[10-11]和感知哈希(Perceptual Hashing)[12-14]这两类技术.这两类技术的特点是对不改变图像内容的编辑(如压缩、去噪等)具有稳健性，但对于会引起内容失真的恶意编辑十分敏感.图像内容认证相关研究成果[15-18]表明，此类技术计算高效、针对性强，能有效地检测篡改并兼容良性编辑，防止恶意用户扭曲图像内容抹黑版权人或图像当事人.内容认证可以限制和约束用户对图像的编辑方式，但不能对编辑用户的身份进行限定，难以实现授权.

数字水印和感知哈希技术较好地实现了图像版权保护和内容认证，却难以快速检测编辑行为的授权性.考虑以下应用场景：某著名摄影师拍摄到一组高清地质图片，并将照片的使用权转让给某科研机构用于学术研究.此后，科研机构将图片作为研究素材投稿至某期刊.为规避纠纷，期刊主编需要对来稿中的图片内容和来源进行甄别.一方面，如果摄影师在图片中嵌入了鲁棒水印，通过提取水印，主编可以较容易地鉴别图片确实是出自摄影师之手而非伪造；另一方面，运用感知哈希或半脆弱水印技术，主编也可以检测图像内容是否被恶意篡改.然而，运用上述方法很难快捷地鉴别图片的编辑或使用是否得到版权人的授权.

数字签名(Digital Signatures)自1978年由Rivest、Shamir和Adleman[19]提出以来，一直是数据认证的重要技术.普通数字签名的特点是签名不可伪造以及签名人行为不可抵赖[20].在上述场景中，如果摄影师对图片进行数字签名并发送给科研机构，科研机构将签名后的图片投稿至期刊，期刊主编的确可以通过验证签名来证实图像确实来自于版权人(摄影师).但普通数字签名满足不可伪造性，对图像的任何编辑都会导致签名验证失败，不支持用户对图像进行编辑，包括良性编辑.总之，单纯使用数字签名进行图像验证，难以实现图像编辑授权.

同态数字签名(Homomorphic Digital Signatures)[21]支持对已认证数据进行再编辑并使其通过验证.与传统数字水印技术相比，公钥密码体制下具有同态性质的数字签名更利于实现图像编辑合法性检测，且基于密码组件构造的方案能获得可证明安全性[22].近年来，基于同态数字签名的图像认证方案取得了一些进展[23-28].

Naveh和Tromer[24]2016年提出一种基于密码组件的可编辑认证方案，该方案利用数字签名与零知识证明技术生成“图像证据”，支持编辑人对认证后图像进行原始签发人允许的编辑，并独立证明编辑后图像的有效性.虽然该方案的安全性较高，但只考虑对编辑行为限制，没有考虑对编辑人身份进行指定，且方案效率较低(针对分辨率为128×128的图像，认证时长306 s，认证公钥占用空间2.6 GB)，实用性有待加强.

Chen等人[26]于2019年提出支持裁剪操作的图像认证方案，该方案基于承诺值等密码学组件设计可截取图像签名，但该方案仅支持裁剪操作，有局限性.在文献[26]方案的基础上，Chen等人[26]2020年提出基于编辑限定的图像认证方案[27-28]，此类方案可以有效地实现图像编辑行为限制与认证，且方案具有通用性，支持多类编辑.但是，上述方案中认证后的图像均为公开可编辑，不支持编辑授权.

总之，现有的研究方案难以同时检测图像编辑行为和用户身份的合法性，从而难以为图像编辑行为的检测提供足够技术支持.图像认证相关技术汇总至表1.

表1 图像版权保护与认证相关技术

相关技术	主要用途	优点	是否支持授权
鲁棒水印	版权声明	稳健、抗攻击	否
半脆弱水印	篡改检测	篡改定位、修复	否
感知哈希	内容认证	高效、有针对性	否
普通数字签名	完整性检测	可检测图像来源	否
同态数字签名	编辑检测	可证明安全	部分支持

1.1 研究思路

本文旨在提出一个有效的图像编辑与举证方案，从技术上检测用户对图像的编辑行为是否经过版权人许可.

现代密码学中的公钥密码体制(非对称密码体制)为本文中的方案设计提供了研究思路.公钥密码体制下的密码算法，对应着一组公私钥对.在使用过程中，公钥公开，私钥保密.公钥密码体制为可授权图像编辑提供了研究思路.

本文设计的方案，为同时实现图像编辑行为限定与编辑用户授权，分别引入版权人公私钥对和编辑人公私钥对. 在图像授权过程中，需要输入版权人私钥和编辑人公钥，实现版权人对特定用户授权且授权行为不可抵赖；另外，在编辑举证过程，需要提供编辑人私钥，实现编辑人身份限定且编辑行为不可抵赖. 验证人只需输入版权人公钥即可方便快捷地验证图像编辑是否经过版权人授权，方案公开可验证. 方案构思示意图如图 1.

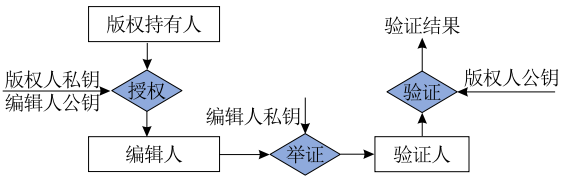


图 1　方案构思示意图

1.2　本文贡献

本文基于公钥密码技术，设计了一种便捷的图像验证方案. 通过该方案，图像接收方可以快捷地验证图像编辑人对图像的编辑或使用是否经过版权人授权. 新方案基于密码技术，首次同时实现了图像编辑方式限定与编辑用户授权，新方案具有以下三个重要性质：

(1) 图像来源可追溯. 图像版权人对图像进行初始认证和授权，版权人对自身授权行为不可抵赖，且图像接受方可借助验证算法验证图像来源以及图像内容是否合法；

(2) 编辑行为可限定. 图像编辑人只有对图像执行版权人许可的编辑，才能使图像通过最后的验证；

(3) 编辑用户可认证. 只有版权人指定的编辑人对图像进行编辑，才能使得图像通过最后的验证. 非授权人，即使按照规则编辑图像，也无法使图像通过验证.

本文主要技术挑战是同时实现图像编辑方式限定和编辑用户授权. 以上图像认证系统的核心组件是一个新功能的聚合器——可认证聚合器. 聚合器(Accumulator，简称 ACC)[29] 属于一种证明系统(Proof system)，用于证明给定集合中成员的归属性. 利用聚合器，可以根据集合 $S=\{s_1,s_2,\cdots,s_n\}$ 有效地生成简要计算结果，该过程称为将集合 S 聚合，简要计算结果称为聚合值. 另外，还可以利用聚合值，有效地为集合中任一元素生成证据 wit_i 以证明元素 $s_i\in S$，该过程称为成员归属证明. 在传统聚合器中，只要满足 $s_i\in S$，则 wit_i 是公开可计算的. 在我们的设计中，借助一组公私钥对，对聚合器算法进行重新设计，在聚合算法中加入公钥，将 wit_i 由公开可计算转变为指定操作人可计算，即只有相应的私钥持有人才能计算 wit_i，即使满足 $x_i\in X$. 该设计也成为图像认证方案中同时实现编辑方式限定和编辑用户授权的重要密码组件，详细设计见本文第 4 节.

2　预备知识

2.1　符号定义

本文设计方案使用的部分通用符号定义见表 2，其他符号定义在文中另有标注.

表 2　算法设计中相关符号定义

参数	含义
$\mathbb{Z}_p$	整数集$[0,p-1]$
$\mathbb{Z}_p^*$	$\mathbb{Z}_p$中与p互素的整数集合
$\mathbb{G}$	循环群$\mathbb{G}$
$\lvert\mathbb{G}\rvert$	群$\mathbb{G}$中元素的个数，即群的阶
sizeof($\mathbb{G}$)	群$\mathbb{G}$中元素的长度数
$\mathcal{BP}$	对称结构的双线性映射($\mathbb{G}_1,\mathbb{G}_2,e,p$)
$\lvert P\rvert$	集合 P 中元素的个数
$\{0,1\}^*$	任意长度的比特串
λ	安全参数
M	图像
pk_A	授权人公钥
pk_E	编辑人公钥
sk_A	授权人私钥
sk_E	编辑人私钥
C	编辑许可证书(Certificate)
π	编辑人输出的证据

2.2　双线性映射[30]

设 λ 为安全参数，p 是不小于 2^λ 的大素数，$\mathbb{G}_1$，$\mathbb{G}_2$ 均为阶为 p 的循环群，双线性映射 $e:\mathbb{G}_1\times\mathbb{G}_2\to\mathbb{G}_T$ 满足以下性质：

(1) 双线性性(Bilinearity). 对于任何元素 $g_1\in\mathbb{G}_1$、$g_2\in\mathbb{G}_2$ 以及 $x,y\in\mathbb{Z}_p$，都有 $e(g_1^x,g_2^y)=e(g_1,g_2)^{xy}$；

(2) 非退化性(Non-degeneracy). 至少存在一组元素 $g_1\in\mathbb{G}_1$、$g_2\in\mathbb{G}_2$，满足 $e(g_1,g_2)\neq1$；

(3) 可计算(Computability). 对于任意的 $g_1\in\mathbb{G}_1$、$g_2\in\mathbb{G}_2$，存在多项式时间的算法计算 $e(g_1,g_2)$.

双线性映射(Bilinear mapping)由五元组($\mathbb{G}_1$，$\mathbb{G}_2$，$\mathbb{G}_T$，e，p)组成. 若$\mathbb{G}_1=\mathbb{G}_2$，为对称映射，否则为非对称映射. 本文中算法构造采用对称双线性映射，并统一写成了($\mathbb{G}_1$，$\mathbb{G}_2$，e，p)，此时的双线性映射表示成 $e:\mathbb{G}_1\times\mathbb{G}_1\to\mathbb{G}_2$.

2.3　困难性问题假设[31]

定义 1.　可忽略函数 negl(x). 如果对于任意多项式 $f(x)$，存在一个正整数 N，使得当 $x>N$ 时有：

$$\mathrm{negl}(x)<\frac{1}{f(x)}.$$

设 g 为循环群 $\mathbb{G}$ 的生成元，$\mathbb{G}$ 上的 CDH(Computational Diffie-Hellman) 困难性假设和 q-SDH (q-Strong Diffie-Hellman)困难性假设的定义如下：

定义 2. CDH 问题. 对于随机选取的 $a,b\in\mathbb{Z}_p^*$，给定 $(g,g^a,g^b)\in\mathbb{G}^3$，计算 g^{ab}.

CDH 问题困难性假设：任何多项式时间的敌手 $\mathcal{A}_{\mathrm{CDH}}$，解决上述 CDH 问题的概率均是可忽略的，即：

$$\Pr[\mathcal{A}_{\mathrm{CDH}}(g^a,g^b)\rightarrow g^{ab}]\leq\mathrm{negl}(\lambda).$$

定义 3. q-SDH 问题. 对于随机选取的 $\alpha\in\mathbb{Z}_p^*$，给定 $(g,g^{\alpha},g^{\alpha^2},\cdots,g^{\alpha^q})\in\mathbb{G}^{q+1}$，找出一个二元组 $(s,g^{\frac{1}{s+\alpha}})$，其中 $s\in\mathbb{Z}_p^*$.

q-SDH 困难性假设. 任何多项式时间的敌手 $\mathcal{A}_{q\text{-SDH}}$，解决上述 q-SDH 问题的概率均是可忽略的问题，即：

$$\Pr[\mathcal{A}_{q\text{-SDH}}(g^{\alpha},g^{\alpha^2},\cdots,g^{\alpha^q})\rightarrow(s,g^{\frac{1}{s+\alpha}})]\leq\mathrm{negl}(\lambda).$$

上述定义中，$\mathrm{negl}(\lambda)$ 是关于安全参数 λ 的可忽略函数.

2.4 数字签名方案及安全模型定义[31]

一个数字签名方案(Digital Signature Scheme)由三个多项式时间的算法构成：

(1) 密钥生成算法 $(pk_s,sk_s)\leftarrow\mathrm{KeyGen}(\lambda)$：输入系统安全参数，输出签名公私钥对 (pk_s,sk_s)；

(2) 签名算法 $\sigma\leftarrow\mathrm{Sign}(sk_s,M)$：输入签名人私钥和待签名数据 M，输出签名 σ；

(3) 验证算法 $0/1\leftarrow\mathrm{Verify}(pk_s,M,\sigma)$：输入签名人公钥 pk_s、数据 M 以及签名 σ，输出验证结果 0 或 1，1 表示验证通过，0 表示验证失败.

标准数字签名方案的安全目标是自适应选择消息攻击下存在性不可伪造(Existentially Unforgeable against Adaptively Chosen Message Attacks，EUF-CMA)，EUF-CMA 安全模型由挑战者和攻击者之间的游戏定义，游戏分为三个阶段：

(1) 系统建立阶段. 挑战者基于安全参数 λ，运行密钥生成算法生成签名公私钥对 (pk_s,sk_s)，并将 pk_s 作为挑战公钥发送给攻击者.

(2) 签名询问阶段. 攻击者自适应地选择一组消息 $\Omega=\{M_i\}_{1\leq i\leq q_s}$，并向挑战者询问消息的签名，其中 q_s 为询问次数.

(3) 输出阶段. 攻击者输出消息签名对 (M^*,σ^*).

在上述游戏中，如果满足

$M^*\notin\Omega$ 且 $\mathrm{Verify}(pk_s,M^*,\sigma^*)=1$，

则攻击者获胜.

定义 4. 对一个数字签名方案而言，如果不存在多项式时间的攻击者，能以不可忽略的概率在上述游戏中获胜，则称其是 EUF-CMA 安全的.

2.5 图像编辑函数定义

现有的图像认证方案中，多数方案依据编辑后图像内容是否发生改变来区分编辑是良性还是恶意，此类区分方法未考虑用户需求，存在一定片面性. 本文方案旨在由图像授权人制定编辑规则，编辑人依照规则编辑图像即为合法编辑，否则认定非法或越权编辑.

参照文献[28]中的描述，本文用集合定义编辑规则. 集合中每个元素代表一种图像编辑行为，可由图像编辑软件 Adobe Photoshop 或函数库 OpenCV 完成. 为形式化定义，将图像编辑方法用 $M_i\leftarrow f_i(M,a_i)$ 表示，其中 f_i 表示图像处理方法(例如 JPEG 压缩)，a_i 表示处理参数(如压缩质量因子 60)，而 M_i 表示处理后的新图像. 特殊情况下，允许 f_i 为空操作，此时 $a_i=\varnothing$，该方法表示不对 M 作任何处理，M_i 等同于原始图像.

这些编辑方法将组成一个集合 $P=\{(f_i,a_i)\}_{1\leq i\leq|P|}$，即需要授权的编辑操作的数目. 集合 P 可用于表示某种编辑规则，集合中的每个元素都对应着一种许可的图像编辑方法. 一幅图像 M 在编辑规则的作用下，会生成一组图像集 $\mathcal{M}=\{M_i\}_{1\leq i\leq n}$(如图 2).

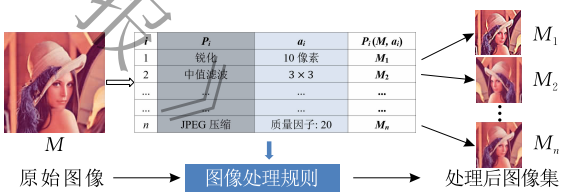


图 2 图像编辑规则定义

3 系统设计与方案安全模型

3.1 系统设计

设计支持图像编辑授权与举证的应用系统将涉及三类操作实体：图像版权所有人(Image Copyright Holder)、图像编辑人(Editor)和图像接收方/验证人(Verifier)，各实体涉及的操作如下：

(1) 图像版权持有人. 制定图像编辑规则并对特定用户进行编辑授权，该实体为诚信实体；

(2) 编辑人. 对图像进行编辑并举证编辑行为的合法性；

(3) 验证人. 验证图像内容是否真实有效，即图像编辑是否经过了授权.

以上系统安全性要求：需要同时满足编辑行为可限定和编辑用户可认证，即只有被授权的用户按照版权人制定的规则编辑图像，才能被认定为合法编辑.

3.2　方案定义与安全模型

3.2.1　方案形式化定义

本节将针对上述应用系统，设计支持图像编辑授权与举证方案(Authorizable Image Editing and Proof，AIEP). 一个 AIEP 方案由五个多项式运行时间的子算法构成，分别是系统设置算法 Setup、密钥生成算法 KeyGen、授权算法 Authorize、编辑举证算法 EditProve 和验证算法 Verify，各子算法形式化定义如下：

(1) $param \leftarrow \mathrm{Setup}(\lambda)$：系统设置算法. 算法输入安全参数 λ，输出系统公开参数 $param$. 算法由图像版权持有人执行；

(2) $((sk_A, pk_A), (sk_E, pk_E)) \leftarrow \mathrm{KeyGen}(param, n)$：密钥生成算法. 算法输入公开参数 $param$ 和非负整数 n，输出授权人公私钥对 (sk_A, pk_A) 和编辑人的公私钥对 (sk_E, pk_E). 算法由版权持有人和授权编辑人各自执行；

(3) $(C, t) \leftarrow \mathrm{Authorize}(sk_A, pk_E, M, P)$：授权算法. 算法输入授权人私钥 sk_A、编辑人公钥 pk_E、图像 M 以及图像编辑规则 P，输出编辑许可证书 C 和编辑令牌 t，其中要求编辑规则中图像编辑方法数 $|P| \leq n$. 该子算法的输出中，证书 C 公开，而令牌 t 将作为保密数据发送给编辑人用于编辑和举证. 算法由图像版权人执行；

(4) $(M', \pi) \leftarrow \mathrm{EditProve}(sk_E, pk_A, M, C, t)$：编辑举证算法. 算法输入编辑人私钥 sk_E、授权人公钥 pk_A、图像 M、编辑许可证书 C 以及编辑令牌 t，输出编辑后的图像 M' 以及其证据 π. 算法由授权编辑人执行；

(5) 验证算法 $\{0,1\} \leftarrow \mathrm{Verify}(pk_A, M', C, \pi)$：算法输入图像授权人公钥 pk_A、编辑后图像 M'、授以证书 C 以及编辑证据 π，输出结果 1 或 0. 其中 1 表示验证成功，0 表示验证失败，该算法由图像验证方执行.

3.2.2　方案正确性要求

上述图像编辑授权与举证方案的正确性要求：基于系统设置和密钥生成算法正确运行的前提下，任何获得授权的编辑人，其依据授权人所定义的编辑规则编辑图像并生成证据，一定会使编辑后图像通过验证，即

若 $param \leftarrow \mathrm{Setup}(\lambda) \wedge$

$((sk_A, pk_A), (sk_E, pk_E)) \leftarrow \mathrm{KeyGen}(param, n) \wedge$

$C \leftarrow \mathrm{Authorize}(sk_A, pk_E, M, P) \wedge$

$(M', \pi) \leftarrow \mathrm{EditProve}(sk_E, pk_A, M, C, t)$，

则 $\mathrm{Verify}(pk_A, M', C, \pi) = 1$.

3.2.3　AIEP 方案安全模型

图像编辑授权与举证方案的安全性要求主要针对两类用户：(1) 授权用户. 要求该类用户无法为违反编辑规则的而编辑的图像计算有效证据，即编辑行为可限定；(2) 非授权用户. 该类型用户无法为任何图像计算有效证据，即使对图像执行的是授权人准许的编辑，即编辑用户可认证. 对一个安全的 AIEP 方案来说，上述要求即使在攻击者能获得大量合法编辑过的图像及有效证据的情况下也应得到满足. 本文将这样的安全性称为自适应选择图像攻击下证据存在性不可伪造(Proof Existentially Unforgeable against Adaptive Chosen Image Attacks，PEU-CIA)安全性.

参照密码学中数字签名方案的安全模型定义(2.3 节)，给出 AIEP 方案的安全模型，针对授权用户和非授权用户，分别用 $\mathrm{PEU\text{-}CIA_a}$ 和 $\mathrm{PEU\text{-}CIA_b}$ 表示.

模型由挑战者和攻击者之间的游戏来定义. 在游戏中，攻击者可以向挑战者自适应性地询问一些按照版权人所允许的编辑方法所产生的图像及其有效性证据. 挑战者如实予以回答. 询问结束后，攻击者输出相应计算结果完成攻击.

(1) $\mathrm{PEU\text{-}CIA_a}$(授权用户)安全模型. 该模型由以下游戏定义，分为三个阶段：

Phase 1. 系统建立阶段. 基于安全参数 λ 和正整数 n，挑战者运行 Setup 和 KeyGen 算法生成公开参数 $param$ 和公私钥对 (sk_A, pk_A)、(sk_E, pk_E). 由于该模型考虑的是授权用户，挑战者需要将 $param$、(pk_A, pk_E) 连同授权编辑用户的私钥 sk_E 一同发送给攻击者.

Phase 2. 编辑许可证书询问. 考虑是授权用户，在此阶段，攻击者可以询问图像许可证书以及对应的编辑令牌. 攻击者自适应地选定一组信息 $\{(M_i, P_i)\}_{1 \leq i \leq q_a}$ 发送给挑战者，挑战者基于上述信息，为每一对 (M_i, P_i) 计算编辑许可证书 C_i 以及编辑令牌 t_i 并发送给攻击者，其中 q_a 是攻击者在此阶段的询问次数.

Phase 3. 输出. 攻击者输出图像以及对应证据(M^*,π^*,C^*).

在上述游戏中,如果对于任意的$i\in[1,q_a]$、$i_j\in[1,|P_i|]$以及$(f_{i_j},a_{i_j})\in P_i$,均满足:

$M^*\neq f_{i_j}(M_i,a_{i_j})$且 Verify$(pk_A,M^*,C^*,\pi^*)=1$,

则攻击者获胜.

定义 5. 编辑行为可限定. 如果不存在多项式时间的攻击者,能以不可忽略的概率在上述游戏中获胜,则称 AIEP 方案是编辑行为可限定的.

(2) PEU-CIA$_b$(非授权用户)安全模型定义的游戏分为四个阶段:

Phase 1. 系统建立阶段. 基于安全参数λ和正整数n,挑战者运行 Setup 和 KeyGen 算法生成公开参数 $param$ 和公私钥对(sk_A,pk_A)、(sk_E,pk_E). 对于非授权用户,挑战者只需将公钥(pk_A,pk_E)和公开参数 $param$ 发送给攻击者.

Phase 2. 编辑许可证书询问. 考虑是非授权用户,在此阶段,攻击者可以询问图像的编辑许可证书,但不可以询问编辑令牌. 攻击者自适应地选定一组信息$\{(M_i,P_i)\}_{1\leq i\leq q_1}$发送给挑战者,挑战者基于上述信息,为每一对$(M_i,P_i)$计算编辑许可证书$C_i$并发送给攻击者,其中$q_1$是攻击者在此阶段的询问次数.

Phase 3. 证据询问. 攻击者还可以基于图像的编辑证书,询问图像的编辑证据. 攻击者自适应地选定一组信息$\{(M_j,C_j)\}_{1\leq j\leq q_2}$发送给挑战者,挑战者基于上述信息,为每一对$(M_j,C_j)$计算编辑证据$\pi_j$并发送给攻击者,其中$q_2$攻击者在此阶段的询问次数.

Phase 4. 输出. 攻击者输出图像以及对应证据(M^*,π^*,C^*).

在上述游戏中,如果对于任意的j都满足$M^*\neq f_{j_i}(M_j,a_{j_i})$,则现有模型是上一模型的特例,因此,只考虑如下情况:对于任意的$j\in[1,q_2]$,存在$j_i\in[1,|P_j|]$以及$(f_{j_i},a_{j_i})\in P_j$,满足:

$$M^*\neq M_j\text{且}M^*=f_{j_i}(M_j,a_{j_i})\text{且}$$
$$\text{Verify}(pk_A,M^*,C^*,\pi^*)=1,$$

则攻击者获胜.

定义 6. 如果不存在多项式时间的攻击者,能以不可忽略的概率在上述游戏中获胜,则称 AIEP 方案是编辑用户可认证的.

定义 7. 如果一个 AIEP 方案同时满足编辑行为可限定和编辑用户可认证,那么称其是 PEU-CIA 安全的.

4 算法详细设计

4.1 算法构造

根据 3.2.1 节方案形式化定义,一个 AIEP 方案由五个多项式运行时间的子算法构成,分别是 Setup、KeyGen、Authorize、EditProve 和 Verify. 下文以双线性映射为基础组件构造 AIEP 方案.

算法 1. 系统设置算法 Setup.

输入:安全参数λ

输出:公开参数 $param$

S1. 选择对称结构的双线性群$\mathcal{BP}=(\mathbb{G}_1,\mathbb{G}_2,e,p)$,其中$p$为大素数且$p>2^\lambda$;

S2. 随机选择生成元$g\in\mathbb{G}_1$;

S3. 选择哈希函数$H_1:\{0,1\}^*\rightarrow\mathbb{Z}_p$,$H_2:\{0,1\}^*\rightarrow\mathbb{G}_1$;

S4. 设置公开参数$param=\{g,H_1,H_2,\mathcal{BP}\}$;

S5. RETURN $param$;

算法 2. 密钥生成算法 KeyGen.

输入:公开参数 $param$ 和正整数n

输出:授权人公私钥对(pk_A,sk_A)以及编辑人公私钥对(pk_E,sk_E)

G1. 版权人选取随机数$x,y\in\mathbb{Z}_p^*$;编辑人选取$u\in\mathbb{Z}_p^*$;

G2. 版权人设置$sk_A=(x,y)$;编辑人设置$sk_E=u$;

G3. 版权人计算$Y=g^y$;编辑人计算$U=g^u$;

G4. 版权人计算 FOR $i=0$ to n $X_i=g^{x^i}$;

G5. 版权人设置$pk_A=(\{X_i\mid 0\leq i\leq n\},Y)$,编辑人设置$pk_E=U$;

G6. RETURN $((sk_A,pk_A),(sk_E,pk_E))$;

算法 3. 授权算法 Authorize.

输入:授权人私钥sk_A、编辑人公钥pk_E、图像M、编辑规则P

输出:图像编辑证书C和编辑令牌t

A1. FOR $i=0$ to $|P|$ //基于图像编辑规则计算图像哈希

A2. $M_i=f_i(M_i,a_i)$; //编辑图像

A3. $h_i=H_1(M_i)$; //哈希计算

A4. 选择随机数$r\in\mathbb{Z}_p^*$并计算

$$A=g^{u\cdot r\prod_{i=1}^{|P|}(h_i+x)}=(U)^{r\prod_{i=1}^{|P|}(h_i+x)};$$

A5. 计算$\sigma=(H_2(A))^y$;

A6. 设置编辑令牌$t=\{\{h_i\}_{1\leq i\leq|p|},r\}$;

A7. 设置$C=(A,\sigma)$;

A8. RETURN (C,t);

算法 4. 编辑算法 EditProve.

输入:编辑人私钥sk_E、授权人公钥pk_A、编辑证书C,编辑令牌t和图像M

输出:图像证据π和编辑后图像M'

E1. IF $e(\sigma,g)\neq e(H_2(A),Y)$

E2.　RETURN ∅；

E3. 从 P 中选取规则(f_i,a_i)计算 $M'=f_i(M_i,a_i)$；

E4. 对新图像 M'进行哈希计算 $h_i=H_1(M')$

E5. 计算 $\pi=g^{u\cdot t\prod_{j=1,j\neq i}^{|P|}(h_j+x)}=[g^{\prod_{j=1,j\neq i}^{|P|}(h_j+x)}]^{u\cdot t}$

E6. RETURN (M',π)；

算法 5.　验证算法 Verify.

输入：授权人公钥 pk_A、图像证据 π、编辑证书 C、编辑后图像 M'

输出：0/1

V1. 对待验证图像 M'进行哈希计算 $h_i=H_1(M')$；

V2. IF $e(\sigma,g)=e(H_2(A),Y)$且 $e(\pi,g^x g^{h_i})=e(A,g)$

V3.　RETURN 1；

V4. ELSE

V5.　RETURN 0；

4.2　正确性分析

根据算法构造，如果有如下等式

$$e(\sigma,g)=e(H_2(A)^y,g)=e(H_2(A),g^y)\quad(1)$$

以及

$$\begin{aligned}e(\pi,g^x g^{h_i})&=e(g^{ur\prod_{j=1,j\neq i}^{|P|}(h_j+x)},g^x g^{h_i})\\&=e(g^{ur\prod_{j=1,j\neq i}^{|P|}(h_j+x)},g^{h_i+x})\\&=e(g^{ur\prod_{j=1}^{|P|}(h_j+x)},g)=e(A,g)\end{aligned}\quad(2)$$

因此，Verify$(pk_A,M',C,\pi)=1$，即在正确生成密钥的前提下，由授权算法正确计算出的编辑证书结合编辑举证算法正确计出证据，可以使得图像通过验证.

5　方案安全性分析

在应用系统中，系统安全性由数据传输安全性与方案构造安全性共同保证. 数据的传输分为两种信道：公开信道和秘密信道. 秘密信道用于传输私密数据，秘密信道数据不泄露的情况下，系统安全性主要取决于方案构造的安全性，本节将分别在 PEU-CIA$_a$和 PEU-CIA$_b$安全模型下，证明方案构造的安全性.

5.1　q-SDH 指数问题、线性 CDH 问题及其困难性

为更好地论证方案的安全性，本节将基于两个标准困难问题假设定义两个新的困难问题：q-SDH 指数问题和线性 CDH 问题.

定义 8.　q-SDH 指数问题. 对于随机选取的 $\alpha\in\mathbb{Z}_p^*$，给定$(\beta,g,g^\alpha,g^{\alpha^2},\cdots,g^{\alpha^q})\in\mathbb{Z}_p^*\times\mathbb{G}_1^{q+1}$，找出一个二元组$(s,g^{\frac{\beta}{s+\alpha}})$，其中 $s\in\mathbb{Z}_p^*$.

引理 1.　q-SDH 指数问题的困难性与传统 q-SDH 问题困难性等价.

证明.

(1) 如果传统 q-SDH 问题易解，则 q-SDH 指数问题易解，分析如下：

假设 q-SDH 问题易解，则给定$(g,g^\alpha,g^{\alpha^2},\cdots,g^{\alpha^q})\in\mathbb{G}_1^{q+1}$，可容易地找出$(s,g^{\frac{1}{s+\alpha}})$. 结合 q-SDH 指数问题的输入，利用 β 可计算出：$g^{\frac{\beta}{s+\alpha}}=(g^{\frac{1}{s+\alpha}})^\beta$，并输出二元组$(s,g^{\frac{\beta}{s+\alpha}})$，于是 q-SDH 指数问题易解.

(2) 如果 q-SDH 指数问题易解，则传统 q-SDH 问题易解. 分析如下：

假设 q-SDH 指数问题易解，则给定$(\beta,g,g^\alpha,g^{\alpha^2},\cdots,g^{\alpha^q})\in\mathbb{Z}_p^*\times\mathbb{G}_1^{q+1}$，可容易地找出$(s,g^{\frac{\beta}{s+\alpha}})$，计算 $g^{\frac{1}{s+\alpha}}=(g^{\frac{\beta}{s+\alpha}})^{\beta^{-1}}$，并以二元组$(s,g^{\frac{1}{s+\alpha}})$作为 q-SDH 的解. 于是传统 q-SDH 易解.

综上两点：q-SDH 指数问题的困难性与传统 q-SDH 问题困难性等价.　　证毕.

定义 9.　线性 CDH 问题. 对于随机选取的 $a,b\in\mathbb{Z}_p^*$，给定$(g,g^a,g^b,g^{b^2},\cdots,g^{b^q})\in\mathbb{G}_1^{q+2}$，计算 $g^{a\gamma(b)}$，其中 $\gamma(b)$是关于 b 的次数不高于 q 的某个非平凡多项式.

引理 2.　线性 CDH 问题困难性与传统 CDH 问题困难性等价.

证明.

不失一般性，设 $\gamma(b)=\sum_{i=0}^{n-1}c_i b^n$ 是关于 b 的某个 n 阶随机多项式，其中 $n\leq q$，且 c_i 为多项式系数.

(1) 如果传统 CDH 问题易解，则线性 CDH 问题易解，分析如下：

首先，假设传统 CDH 问题易解，结合线性 CDH 问题的输入$(g,g^a,g^b,g^{b^2},\cdots,g^{b^q})\in\mathbb{G}_1^{q+2}$，可计算$(g^{ab},g^{ab^2},\cdots,g^{ab^q})\in\mathbb{G}_1^q$. 然后，对$(c_1,c_1,\cdots,c_q)\in\mathbb{Z}_p^q$计算

$$g^{a\gamma(b)}=(g^{\sum_{i=0}^{n-1}c_i b^n})^a=\prod_{i=0}^{n}(g^{c_i b^i})^a=\prod_{i=0}^{n}(g^{ab^i})^{c_i},$$

其中 $n\leq q$，从而 $g^{a\gamma(b)}$ 可计算. 于是，线性 CDH 问题易解.

(2) 如果线性 CDH 问题易解，则传统 CDH 问题易解，分析如下：

假设线性 CDH 问题易解，则给定$(g,g^a,g^b,g^{b^2},\cdots,g^{b^q})\in\mathbb{G}_1^{q+2}$，容易计算 $g^{a\gamma(b)}$. 上式中，当$\gamma(b)=b$ 时，$g^{a\gamma(b)}=g^{ab}$，即 CDH 问题是线性 CDH 问题的特例. 于是，CDH 线性问题易解时，CDH 问题易解.

综上两点:线性 CDH 问题困难性与传统 CDH 问题等价. 证毕.

5.2 AIEP 方案安全性分析

本节中,将基于 5.1 节中的定义的两个新的困难问题 q-SDH 指数问题、线性 CDH 问题,分析方案的安全性.

引理 3. 如果 q-SDH 指数问题是困难的,则 AIEP 方案在 PEU-CIA$_a$ 安全模型下是编辑行为可限定的.

证明.

假设在 PEU-CIA$_a$ 模型下,存在多项式攻击算法$\mathcal{A}$以不可忽略的概率攻破 AIEP 方案的编辑用户可授权安全性,则可以构造一个模拟算法$\mathcal{S}_1$,通过与$\mathcal{A}$交互,能以不可忽略的概率解决 q-SDH 指数问题,具体分析如下:

设模拟算法$\mathcal{S}_1$以要解决的 q-SDH 指数问题的实例$(\beta,g,g^{\alpha},g^{\alpha^2},\cdots,g^{\alpha^q})\in\mathbb{Z}_p^*\times\mathbb{G}_1^{q+1}$为输入,目标是输出$(s,g^{\frac{\beta}{s+\alpha}})$,其中 $g\in\mathbb{G}_1$,p 为$\mathbb{G}_1$的阶且 $s\in\mathbb{Z}_p^*$;$\mathcal{S}_1$模拟游戏 PEU-CIA$_a$中的挑战者与攻击者$\mathcal{A}$进行如下交互:

Phase 1. 系统建立阶段. 首先,$\mathcal{S}_1$选取随机数 $y\in\mathbb{Z}_p^*$,计算 $Y=g^y$,并设置 $sk_E=u=\beta$. 其次,$\mathcal{S}_1$令 $g^x=g^{\alpha}$,隐式地设置 $sk_A=x=\alpha$. 由于该模型考虑敌手可以是授权用户,$\mathcal{S}_1$将 $pk_A=(\{g^{b^i}\}_{0\le i\le q},Y)$、$pk_E=U=g^u=g^{\alpha}$以及编辑人的私钥 u 一起发送给$\mathcal{A}$.

Phase 2. 编辑许可证书询问. 首先,$\mathcal{S}_1$新建空的列表 L. 针对$\mathcal{A}$的第 i 次询问(M_i,P_i),$\mathcal{S}_1$选择随机数 $r_i\in\mathbb{Z}_p^*$,设置 $t_i=r_i$,用公钥计算 $A_i=g^{u\cdot t_i\prod_{j_i=1}^{|P_i|}(h_{j_i}+\alpha)}=(g^{\prod_{j_i=1}^{|P_i|}(h_{j_i}+\alpha)})^{\beta\cdot t_i}$. 然后,计算 $\sigma_i=(H_2(A_i))^y$,并将 $C_i=(\{h_{j_i}\}_{1\le j_i\le|P_i|},A_i,\sigma_i)$连同 t_i发送给攻击者,并将(C_i,t_i)加入列表 L. 此阶段$\mathcal{A}$共发起 q_a次询问.

Phase 3. 输出. 攻击者输出图像以及对应证据 (M^*,π^*,C^*).

令多项式 $\psi(x)$是关于 x 的$|P^*|-1$次多项式,由 π^*是 M^*有效的证据可知,一定存在非零整数 d 满足下列等式:

$$\begin{aligned}\pi^*=(A^*)^{\frac{1}{h^*+\alpha}}&=g^{u\cdot t^*\prod_{j=1,j\ne i}^{|P^*|}(h_j+\alpha)}\\&=g^{\frac{\beta t^*\prod_{j=1}^{|P^*|}(h_j+\alpha)}{h^*+\alpha}}=g^{\frac{\beta t^*[(h^*+\alpha)\psi(\alpha)+d]}{h^*+\alpha}}\\&=g^{\beta t^*\psi(\alpha)}g^{\frac{\beta t^*d}{h^*+\alpha}}\end{aligned}\tag{3}$$

上式中,A^*由攻击者输出的伪造 C^*中得到,而 $h^*=H_1(M^*)$. 另外,t^*是与 C^*对应的编辑令牌$\mathcal{S}_1$查询 L 并计算:

$$g^{\frac{\beta}{h^*+\alpha}}=\left(\frac{\pi^*}{g^{\beta t^*\psi(\alpha)}}\right)^{\frac{1}{dt^*}}\tag{4}$$

最后,$\mathcal{S}_1$将$(h^*,g^{\frac{\beta}{h^*+\alpha}})$作为 q-SDH 指数问题的解.

在上述游戏中,由于$\mathcal{S}_1$能以 100% 的概率模拟算法运行并正确回答敌手的询问,则如果存在多项式敌手$\mathcal{A}$以不可忽略的概率 ε_1攻破 AIEP 方案,则可以构造一个模拟算法$\mathcal{S}_1$,通过与$\mathcal{A}$交互,以相同的概率 ε_1解决 q-SDH 指数问题. 由 q-SDH 指数问题的困难性假设(等价于 q-SDH 困难性假设)可知 AIEP 方案在 PEU-CIA$_a$ 安全模型下是编辑行为可限定的. 证毕.

引理 4. 如果线性 CDH 问题是困难的,则 AIEP 方案在 PEU-CIA$_b$ 安全模型下是编辑用户可认证的.

证明.

假设在 PEU-CIA$_b$ 模型下,存在多项式攻击算法$\mathcal{B}$以不可忽略的概率攻破 AIEP 方案的编辑用户可授权安全性,则可以构造一个模拟算法$\mathcal{S}_2$,通过与$\mathcal{B}$交互,能以不可忽略的概率解决线性 CDH 问题.

设模拟算法$\mathcal{S}_2$要解决的线性 CDH 问题的实例$(g,g^a,g^b,g^{b^2},\cdots,g^{b^q})\in\mathbb{G}_1^{q+2}$为输入,目标是输出 $g^{a\gamma(b)}$,其中 p 为$\mathbb{G}_1$的阶,$a,b\in\mathbb{Z}_p^*$ 且 $\gamma(b)$是次数不高于 q 的某个多项式表达式. $\mathcal{S}_2$模拟游戏 PEU-CIA$_b$中的挑战者与攻击者 B 运行如下:

Phase 1. 系统建立. $\mathcal{S}_2$选取随机数 $y\in\mathbb{Z}_p^*$,计算 $Y=g^y$,并隐式地设置 $u=a$ 以及 $x=b$. 最后,S_2将 $pk_A=(\{g^{b^i}\}_{0\le i\le q},Y)$以及 $pk_E=U=g^u=g^a$作为挑战公钥发送给$\mathcal{B}$.

Phase 2. 编辑许可证书询问. 针对$\mathcal{B}$的第 i 次询问(M_i,P_i),$\mathcal{S}_2$选择随机数 $r_i,s\in\mathbb{Z}_p^*$,计算 $A_i=g^{sr_i\prod_{j_i=1}^{|P_i|}(h_{j_i}+b)}=(g^{r_i\prod_{j_i=1}^{|P_i|}(h_{j_i}+b)})^s$和 $\sigma_i=(H_2(A_i))^y$,并设置 $t_i=r_i$. 挑战者新建证书令牌列表 L 保存所有(C_i,t_i),并将 $C_i=(\{h_{j_i}\}_{1\le j_i\le|P_i|},A_i,\sigma_i)$发送给$\mathcal{B}$.

在上述询问阶段,即使 b 未知,借助线性 CDH 问题的实例输入结合多项式分解,A_i是可计算的. 另外,虽然真正的私钥 u 对于挑战者是未知的,从而其无法利用 u 计算出 C_i以回答$\mathcal{B}$的询问,由于 r_i攻击者无法获得,则上述 C_i与利用 u 计算出的证书在形式上不可区分,从而,挑战者的模拟行为与真实算法

运行在计算上不可区分.

Phase 3. 证据询问. 攻击者自适应地选定一组信息$\{(M_j,C_j)_{1\le j\le q_2}\}$发送给挑战者，其中$C_j$来自于攻者在上一阶段询问中获得的信息. 挑战者查询证书令牌列表L，找出C_j对应的令牌信息t_j并计算编辑证据$\pi_j=g^{s\cdot t_j\prod_{j=1,h_j\neq h}^{|P_j|}(h_{j_i}+b)}=\left[g^{j_i=1,h_{j_i}\neq h}\right]^{s\cdot t_j}$.

由于令牌信息与证书是匹配的，上述证据是基于(M_j,C_j)产生的有效证据.

Phase 4. 输出. 攻击者输出图像证据对(M^*,π^*,C^*).

由于π^*是M^*有效的证据，则

$$\pi^*=U^{r^*\prod_{j=1,h_j^*\neq h}^{|P^*|}(h_j^*+x)}=g^{ar^*\prod_{j=1,h_j^*\neq h}^{|P^*|}(h_j^*+b)}.$$

其中$r^*\prod_{j=1,h_j^*\neq h}^{|P^*|}(h_j^*+b)$是关于$b$的$|P^*|-1$次多项式表达式. 挑战者选择$\pi^*$作为线性 CDH 问题的解.

在上述游戏中，由于$\mathcal{S}_2$能以 100% 的概率模拟算法运行并正确回答敌手的询问，则如果存在多项式法$\mathcal{B}$以不可忽略的概率ε_2攻破 AIEP 方案，则可以构造一个模拟算法$\mathcal{S}_2$，通过与$\mathcal{B}$交互，以相同的概率ε_2解决解决线性 CDH 问题. 由线性 CDH 问题是困难性假设可知 AIEP 方案在 PEU-CIA$_b$安全模型下是编辑用户可认证的.　　证毕.

根据定义 7，在q-SDH 指数问题困难性及线性 CDH 问题困难性假设下，我们的 AIEP 方案是 PEU-CIA 安全的，即在自适应选择图像攻击下是证据存在性不可伪造的.

6　实验仿真与性能分析

6.1　总体性能分析

首先，结合方案的构造，对方案的计算开销和传输开销进行分析. 忽略常规图像处理操作时间，方案的效率将主要取决于图像编辑种类n的大小. 方案中各子算法的时间和空间复杂性汇总如表 3.

表 3　方案中各子算法的时间和空间复杂性

算法	时间复杂性	空间复杂性
KeyGen	$O(n)$	$O(n)$
Authorize	$O(n)$	$O(n)$
EditProve	$O(n)$	$O(1)$
Verify	$O(1)$	$O(1)$

不同于传统计算机算法，基于公钥密码组件构造的方案，由于运算基于特殊代数结构(双线性群)，针对于同样的时间复杂性，其计算和传输代价均要大于普通线性数据结构，以获得很高的安全性. 在下面的分析中，我们将主要分析方案中密码组件(包括哈希函数)的计算代价. 方案主要涉及四类耗时较大的群上哈希或代数运算，具体描述如下：

(1) 哈希运算$H_2:\{0,1\}^*\to\mathbb{G}_1$；

(2) $\mathbb{G}_1$群上乘法运算$M_{\mathbb{G}_1}$；

(3) $\mathbb{G}_1$群上指数运算$E_{\mathbb{G}_1}$；

(4) 双线性群上的$pairing$运算$P_{\mathcal{BP}}$.

另外，方案中需要授权的图像的编辑种类也会对方案的计算和传输开销产生影响. 设编辑类种为n，方案的计算和传输开销汇总至表 4 与表 5.

表 4　方案计算开销

算法	计算开销
KeyGen	$(n+3)E_{\mathbb{G}_1}$
Authorize	$(n+1)M_{\mathbb{G}_1}+E_{\mathbb{G}_1}+H_2$
EditProve	$(n+1)M_{\mathbb{G}_1}+nE_{\mathbb{G}_1}+2P_{\mathcal{BP}}$
Verify	$M_{\mathbb{G}_1}+E_{\mathbb{G}_1}+H_2+4P_{\mathcal{BP}}$

表 5　方案存储开销

算法	存储开销
KeyGen	$(n+4)\cdot$sizeof($\mathbb{G}$)
Authorize	2sizeof($\mathbb{G}_1$)+$(n+1)\cdot$sizeof($\mathbb{Z}_p$)
EditProve	sizeof($\mathbb{G}_1$)
Verify	—

由表 4 可知，方案中密钥生成算法所涉及的指数运算最多，因此该子算法是方案中最耗时的算法. 但密钥生成算法仅需要运行一次，生成的密钥可用于多次编辑认证，在实际应用中，对系统整体运行效率的影响较小. 方案的额外存储开销与图像大小无关，在忽略普通整数存储空间的情况下，只与编辑种类n、所选用的双线性群$\mathbb{G}_1$中元素的大小sizeof($\mathbb{G}_1$)以及大整数长度 sizeof($\mathbb{Z}_p$)有关. 这是由于待认证的图像在编辑后生成的新图像均被哈希成了定长的字符串，从而获得一个简短且定长的认证码.

由表 5 可知，密钥生成算法和授权算法的存储开销基于编辑种类线性增长，而编辑举证算法仅需一个群元素大小的存储空间.

6.2　性能测试

为进一步测评方案的效率，本节利用计算机对算法的运行效率进行了详细的测试. 实验设备是一台普通的联想笔记本电脑(型号：ThinkPad X390)，配备 3.4GHz Intel i5-7500 双核中央处理器(CPU)，码专用测试库 GNU Multiple Precision Arithmetic (GMP) Library 和 Pairing-Based Cryptography(PBC) Library 完成，程序代码由 Visual Studio 2017 编译

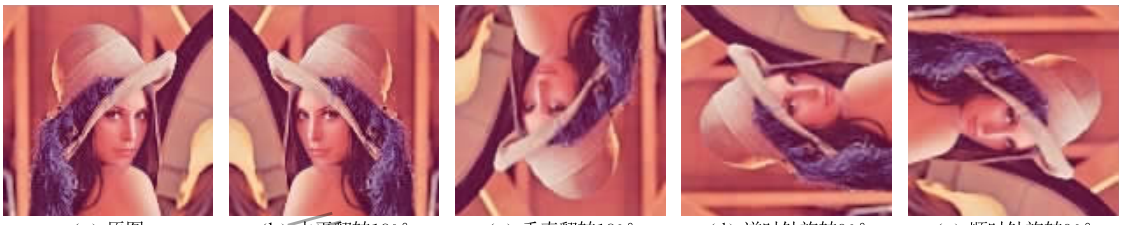
并在 Win10 操作系统上运行.方案选取 PBC 中对称曲线 Curve A 进行了测试,曲线参数如表 6.

表 6 PBC 库曲线技术参数

曲线	群元素大小	安全级别/bit
Curve A	$(\mathbb{G}_1,\mathbb{G}_1,\mathbb{G}_2)$:(512,512,1024)	80
	$(\mathbb{G}_1,\mathbb{G}_1,\mathbb{G}_2)$:(1024,1024,2048)	112

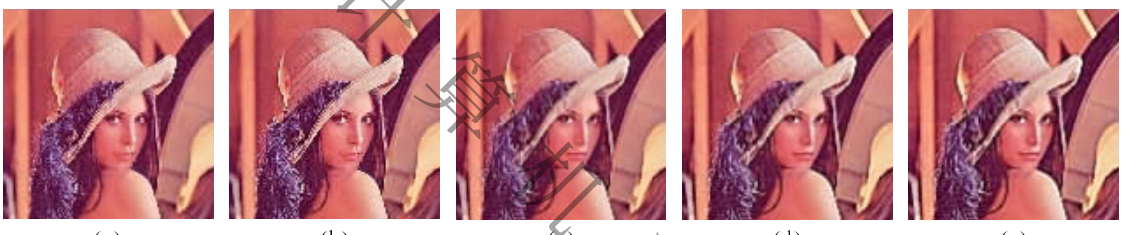
实验图像选取图像 Lenna(分辨率 512×512),分别取 $n=10\sim400$ 进行测试,增长粒度 10,测试数据共 40 组,在 80-bit 安全级别下,方案中各子算法的运行时间如图 6、图 7 所示.由图 6 可知,密钥生成算法时间消耗最大并随着编辑次数 n 的增大呈线性增长,但由于密钥生成算法在一次授权操作中只需要运行一次,对系统效率的影响有限.实验具体操作如下:

首先,利用 Photoshop 将原始图像编辑成 400 张新图像,编辑方式包括常用的锐化、去噪、压缩等.由于篇幅限制,仅列出其中几组编辑结果图 3、图 4 以及图 5.

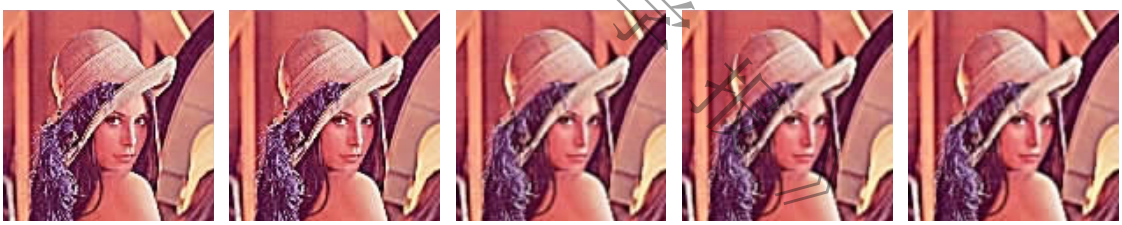


(a) 原图 (b) 水平翻转180° (c) 垂直翻转180° (d) 逆时针旋转90° (e) 顺时针旋转90°

图 3 图像旋转与翻转操作

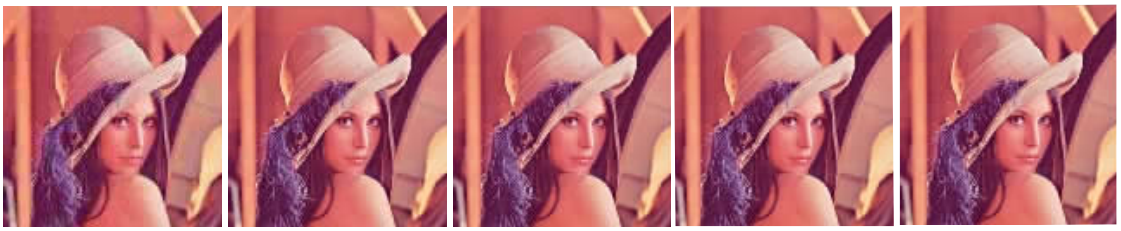


(a) (b) (c) (d) (e)



(f) (g) (h) (i) (j)

图 4 图像锐化操作((a)~(j)锐化等级从 1 到 10,每图递增 1 像素)



(a) (b) (c) (d) (e)

图 5 图像 JPEG 压缩((a)~(e)压缩质量因子分别为 10、20、40、60、80)

其次,再将编辑后的图像进行哈希运算生成图像哈希集.本文对图像进行哈希的方法是:将图像以二进制形式读取,再利用 PBC 中哈希函数将图像比特流映射成群$\mathbb{G}_1$上的元素.此种方法进行图像哈希运算相对于其他子算法是高效的,对方案效率不会形成牵制.

最后,将图像哈希集进行聚合运算并签名,生成图像编辑证据并验证.

为了更直观地反映各子算法的运行时间,针对特定编辑次数($n=10,100,200,300,400$)以及不同的安全级别(80-bit 和 112-bit 安全)对各子算法的运行时间进行了统计,统计结果如表 7、表 8.

表 7　方案运行时间(80-bit 安全)

编辑次数	图像哈希/ms	密钥生成/ms	授权算法/ms	编辑举证/ms	验证/ms
10	1	63	27	1	17
100	13	288	39	10	17
200	31	630	61	27	20
300	43	871	71	42	18
400	71	1384	104	72	18

表 8　方案运行时间(112-bit 安全)

编辑次数	图像哈希/ms	密钥生成/ms	授权算法/ms	编辑举证/ms	验证/ms
10	2	136	59	2	36
100	25	660	77	23	35
200	50	1500	116	55	38
300	76	1861	152	92	37
400	112	2794	226	153	39

由图 6、图 7 所示，我们方案的计算开销主要来源于四个子算法，分别是：密钥生成算法“KeyGen”、授权算法“Authorize”、编辑算法“EditProve”和验证算法“Verify”. 其中“KeyGen”算法耗时较大，但这并不影响方案的整体性能，主要原因如下：上述几个子算法涉及的运行实体有图像版权所有人、编辑人和验证人.

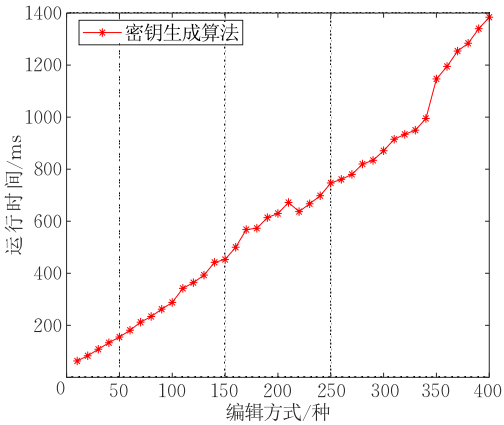


图 6　80-bit 安全密钥生成算法运行时间

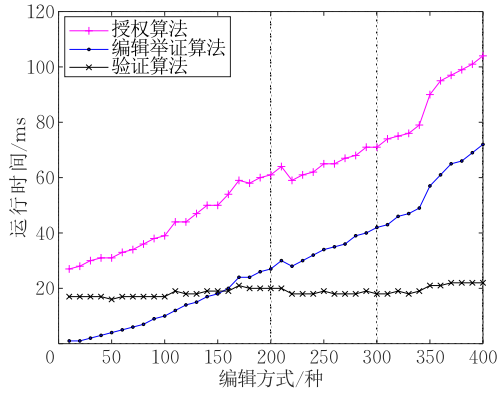


图 7　80-bit 安全授权、举证以及验证算法运行时间

在认证开始之前，图像版权人和编辑人可各自运行“KeyGen”算法中的相关代码生成各自所需密钥，然后将公钥公开，并将私钥保存. 该工作可由线下完成，且只执行一次，不需要与其他实体进行任何交互. 当版权人需要向特定编辑人进行编辑授权时，其利用已生成的密钥运行授权算法后，将授权凭证发送给编辑人，至此，授权工作结束. 如果编辑权限不需要更新或修改，授权算法也只需要运行一次. 编辑人收到授权凭证后，可将凭证保存并重复利用. 当编辑人需要使用和编辑图像时，其编辑图像后可借助授权凭证计算编辑证据，并将证据提供给验证人. 验证人基于证据验证图像的有效性. 在此过程中，只有编辑算法“EditProve”和验证算法“Verify”需要多次运行，而“KeyGen”和“Authorize”只需要运行一次，且“KeyGen”可线下完成.

由表 8 可知，在 112-bit 安全级别下，当编辑次数为 400 次时，这四个子算法的运行时间分别为 2794 ms、226 ms、153 ms 和 39 ms. 这其中，虽然密钥生成算法相对比较耗时，但它可线下完成，且只运行一次. 而其他子算法，特别需要频繁调用的“EditProve”和“Verify”算法是高效的. 另外，方案的验证算法为恒定时间，与编辑种类无关且不超过 40 ms，对于普通应用场景下的图片接受方而言，足以快捷高效地验证图像编辑是否经了授权，且验证过程不需要与授权人和编辑人进行交互.

另外，由表 7、表 8 可知，相对于 80-bit 安全级别，112-bit 安全级别各子算法(包括图像哈希)的运行时间大约是 80-bit 安全级别的 2 倍多，但依然是高效实用的. 图 6、图 7 展现各子算法与编辑种类 n 所呈的线性关系，针对 400 种编辑行为，80-bit 安全级别下授权算法计算时间大约为 100 ms，编辑举证大约需 70 ms(比密钥生成算法的计算时间要少很多)，且方案可证明安全，可以满足需要提供安全保障的图像应用需求.

现有的基于密码技术的图像认证方案中，编辑方式限定是主要设计目标，代表性方案是文献[24]. 但该方案基于零知识证明设计，方案的效率取决于 Gate 的设计数量，当编辑方式相对复杂时，效率难以满足实际应用需求. 文献[28]对密码组件重新设计，在实现类似功能的基础上，大大提升了系统效率，让密码学图像认证方案有了实用价值. 但是，文献[24]和[28]均未能实现图像认证中用户授权功能，本文基于上述方案，在无显著效率降低的前提下，同时实现了编辑方式限定和编辑人身份指定，获取了更有价值的图像认证功能. 相关性能对比见表 9.

表 9 与文献[28]中方案的性能对比(80-bit)

方案	门数	编辑次数	密钥生成/ms	(授权/认证)/ms	编辑举证/ms	验证/ms
[24]	12531999	—	376000	306000		500
[28]	—	400	1384	104	72	18
本文方案			1536	112	88	22

注:以上表格中,关于文献[24]的实验数据摘自原文,其他数据在与文献[24]相同的实验环境中模拟获取.

7 扩 展

由于本文方案设计的主要目的是为图像使用协议提供技术检测方法,考虑到协议的签署方是一对一的,文中方案设计成了单用户授权.然而,在本文工作的基础上,基于支持群体授权的高级密码组件,如属性基加密方案(Attributed-Based Encryption,ABE)[32-33],可以方便快捷地将文中方案扩展成多用户授权方案.

以基于密文策略的属性基加密方案(Ciphertext-Policy Attribute-Based Encryption,CP-ABE)[33]为例.首先,可信授权中心管理一组用户属性,并基于用户属性集生成用户解密私钥;然后,数据共享方制定访问策略并基于该策略加密数据;最后,所有满足访问控制策略的用户均可借助用户解密私钥对密文解密并得到正确的明文.通过 CP-ABE 方案,可基于用户属性实现多用户解密授权.将上述机制用于图像认证,有助于设计基于用户属性的多用户图像编辑授权方案.由于多用户授权不是本文研究的重点,且受限于篇幅,在此仅给出一个基础设计框架(图 8).

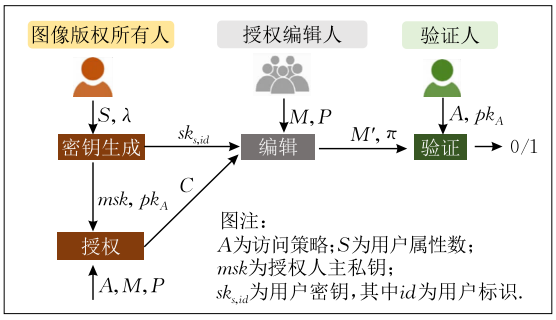


图 8 基于属性的多用户图像编辑授权系统框架图

在对文中方案进行多用户授权扩展时,基于属性的用户授权并不是唯一选择.公钥密码体系中支持多用户操作的高级组件,如基于策略的数字签名(Policy-Based Signatures)[34]、环签名(Ring Signatures)[35]、群签名(Group Signatures)[36-37]、秘密分享方案(Secret Sharing)[38]等都可以与文中方案结合用于实现多用户授权.总之,有了本文工作的基础,实现多用户图像编辑授权是切实可行的.

8 结 论

本文基于公钥密码组件,构造了支持编辑授权与验证的图像认证方案.该方案允许图像授权人对待授权的图像进行初始认证并生成编辑许可证书;图像编辑人基于授权凭证编辑图像并举证编辑行为的合法性;图像接收方(验证人)通过授权人和编辑人提供的证据验证图像.新方案可为图像授权行为提供快捷的检测方法,便于图像接受方在发布图像之前,对图像是否已获得授权进行检测,从技术上规避侵权行为.

方案的优点是:(1)同时实现编辑行为限定和编辑用户认证.只有授权人指定的用户按指定编辑方式编辑图像,才能为编辑后的图像生成有效证据使其通过验证;(2)方案可证明安全.基于密码组件双线性群构造,在既定安全模型下,安全性可归约到密码学困难问题 CDH 问题和 q-SDH 问题;(3)快捷验证.实验数据表明,算法的验证效率可达常数时间,不受图像大小以及授权编辑数目的影响.

虽然本文方案解决了图像认证中的一些关键问题,但仍存在少许不足.比如,公钥的计算和存储开销较大,与编辑种类的增长呈线性关系;但由于密钥生成算法仅运行一次且可线下完成,因此密钥生成算法的计算开销并不会拖累系统的整体性能.另外,公钥不需要传输,且每增加一种编辑方式,公钥只增加一个群元素长度,不会给公钥存储带来困扰.总之,文中方案设计有望成为除版权保护和内容认证外,又一与图像安全应用密切相关的实用型研究.另外,本文还给出了支持多用户授权的扩展设计基础框架,为研究功能更丰富的图像编辑授权方案提供了解决思路.

致 谢 感谢所有匿名审稿人为本文提出的专业宝贵的修改意见,同时,本文写作过程中引用了大量文献和数据资料,也一并向引用文献中提及以及未提及的原创者表示感谢!

参 考 文 献

[1] Dictionaries O. Oxford Portuguese Mini Dictionary. New York, USA: Oxford University Press, 2012

[2] Van Schyndel R G, Tirkel A Z, Osborne C F. A digital watermark//Proceedings of the 1st International Conference on Image Processing. Austin, USA, 1994, 2: 86-90

[3] Van Schyndel R G, Tirkel A Z, Svalbe I D. Key independent watermark detection//Proceedings of the IEEE International Conference on Multimedia Computing and Systems. Florence, Italy, 1999, 1: 580-585

[4] Barni M, Bartolini F, Furon T. A general framework for robust watermarking security. Signal Processing, 2003, 83(10): 2069-2084

[5] Malvar H S, Florêncio D A F. Improved spread spectrum: A new modulation technique for robust watermarking. IEEE Transactions on Signal Processing, 2003, 51(4): 898-905

[6] Singh R, Ashok A. An optimized robust watermarking technique using CKGSA in frequency domain. Journal of Information Security and Applications, 2021, 58: 102734

[7] Abdulrahman A K, Ozturk S. A novel hybrid DCT and DWT based robust watermarking algorithm for color images. Multimedia Tools and Applications, 2019, 78(12): 17027-17049

[8] Huang Ji-Wu, Yun Q Shi, Yao Ruo-He. Adaptive image watermarking based on block classification. Journal of Image and Graphics, 1999, 4(8): 640-643(in Chinese)
(黄继武, Yun Q Shi, 姚若河. 基于块分类的自适应图象水印算法. 中国图象图形学报, 1999, 4(8): 640-643)

[9] Shen Chang-Xiang, Zhang Huan-Guo, Feng Deng-Guo, et al. An overview of information security. Science China (Information Sciences), 2007, 37(2): 129-150(in Chinese)
(沈昌祥, 张焕国, 冯登国等. 信息安全综述. 中国科学(E辑: 信息科学), 2007, 37(2): 129-150)

[10] Haouzia A, Noumeir R. Methods for image authentication: A survey. Multimedia Tools and Applications, 2008, 39(1): 1-46

[11] Rey C, Dugelay J L. A survey of watermarking algorithms for image authentication. Journal on Advances in Signal Processing, 2002, 2002(6): 1-9

[12] Venkatesan R, Koon S M, Jakubowski M H, et al. Robust image hashing//Proceedings of the 2000 International Conference on Image Processing (Cat. No. 00CH37101). Vancouver, Canada, 2000, 3: 664-666

[13] Swaminathan A, Mao Y, Wu M. Robust and secure image hashing. IEEE Transactions on Information Forensics and Security, 2006, 1(2): 215-230

[14] Niu Xia-Mu, Jiao Yu-Hua. An overview of perceptual hashing. Acta Electronica Sinica, 2008, 36(7): 1405-1411 (in Chinese)
(牛夏牧, 焦玉华. 感知哈希综述. 电子学报, 2008, 36(7): 1405-1411)

[15] Tian L, Dai H, Li C. A semi-fragile video watermarking algorithm based on chromatic residual DCT. Multimedia Tools and Applications, 2020, 79(3): 1759-1779

[16] Qin C, Chen X, Luo X, et al. Perceptual image hashing via dual-cross pattern encoding and salient structure detection. Information Sciences, 2018, 423: 284-302

[17] Sajjad M, Haq I U, Lloret J, et al. Robust image hashing based efficient authentication for smart industrial environment. IEEE Transactions on Industrial Informatics, 2019, 15(12): 6541-6550

[18] Chen Fan, He Hong-Jie, Wang Hong-Xia. Variable-payload self-recovery watermarking scheme for digital image authentication. Chinese Journal of Computers, 2012, 35(1): 154-162 (in Chinese)
(陈帆, 和红杰, 王宏霞. 用于图像认证的变容量恢复水印算法. 计算机学报, 2012, 35(1): 154-162)

[19] Rivest R L, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 1978, 21(2): 120-126

[20] Katz J, Lindell Y. Introduction to Modern Cryptography. Boca Raton, USA: CRC Press, 2020

[21] Johnson R, Molnar D, Song D, et al. Homomorphic signature schemes//Proceedings of the 7th International Workshop on Theory and Practice in Public Key Cryptography, Singapore, 2004: 244-262

[22] Feng Deng-Guo. Research on theory and approach of provable security. Journal of Software, 2005, 16(10): 1743-1756(in Chinese)
(冯登国. 可证明安全性理论与方法研究. 软件学报, 2005, 16(10): 1743-1756)

[23] Lin C Y, Chang S F. A robust image authentication method distinguishing JPEG compression from malicious manipulation. IEEE Transactions on Circuits and Systems for Video Technology, 2001, 11(2): 153-168

[24] Naveh A, Tromer E. PhotoProof: Cryptographic image authentication for any set of permissible transformations//Proceedings of the 2016 IEEE Symposium on Security and Privacy (SP). San Jose, USA, 2016: 255-271

[25] Kim J, Lee S, Yoon J, et al. PASS: Privacy aware secure signature scheme for surveillance systems//Proceedings of the 14th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS). Lecce, Italy, 2017: 1-6

[26] Chen H, Wang S, Zhang H, et al. Image authentication for permissible cropping//Proceedings of the 14th International Conference on Information Security and Cryptology. Fuzhou, China, 2018: 308-325

[27] Chen H, Huang X, Wu W, et al. Privacy-aware image authentication from cryptographic primitives. The Computer Journal, 2021, 64(8): 1178-1192

[28] Chen H, Huang X, Wu W, et al. Efficient and secure image authentication with robustness and versatility. Science China Information Sciences, 2020, 63(12): 1-18

[29] Nguyen L. Accumulators from bilinear pairings and applications //Proceedings of the Cryptographers' Track at the RSA Conference 2005. San Francisco, USA, 2005: 275-292

[30] Zhang F, Safavi-Naini R, Susilo W. An efficient signature scheme from bilinear pairings and its applications//Proceedings of the 7th International Workshop on Theory and Practice in Public Key Cryptography. Singapore, 2004: 277-290

[31] Guo F, Susilo W, Mu Y. Introduction to Security Reduction. Cham, Switzerland: Springer, 2018

[32] Goyal V, Pandey O, Sahai A, et al. Attribute-based encryption for fine-grained access control of encrypted data// Proceedings of the 13th ACM Conference on Computer and Communications Security. Alexandria Virginia, USA, 2006: 89-98

[33] Ning J, Cao Z, Dong X, et al. Large universe ciphertext-policy attribute-based encryption with white-box traceability// Proceedings of the 19th European Symposium on Research in Computer Security. Wroclaw, Poland, 2014: 55-72

[34] Bellare M, Fuchsbauer G. Policy-based signatures//Proceedings of the 17th International Conference on Practice and Theory in Public-Key Cryptography. Buenos Aires, Argentina, 2014: 520-537

[35] Karnin E, Bender A, Katz J, Morselli R. Ring signatures: Stronger definitions, and constructions without random oracles //Proceedings of the 3rd Theory of Cryptography Conference. New York, USA, 2006: 60-79

[36] Chaum D, Van Heyst E. Group signatures//Proceedings of the 1991 Workshop on the Theory and Application of Cryptographic Techniques. Springer, Brighton, UK, 1991: 257-265

[37] Boneh D, Boyen X, Shacham H. Short group signatures// Proceedings of the 24th Annual International Cryptology Conference. Santa Barbara, USA, 2004: 41-55

[38] Greene J, Hellman M. On secret sharing systems. IEEE Transactions on Information Theory, 1983, 29(1): 35-41

CHEN Hai-Xia, Ph. D. Her research interests include information security and image authentication.

HUANG Xin-Yi, Ph. D., professor, Ph. D. supervisor. His research interests include cryptography and information security.

ZHANG Fu-Tai, Ph. D., professor, Ph. D. supervisor. His research interests include cryptography and information security.

NING Jian-Ting, Ph. D., professor. His research interests include public-key cryptography and information security.

SONG Yong-Cheng, Ph. D. His research interests include code-based cryptography and information security.

Background

Work of this paper refers to technology of image authentication, an import branch of research on image security and forensics. The aims of image authentication are detection of image integrity and authenticity for image applications in a digital society. There have been plenty of research work in this field. Fragile watermarking and perceptual hashing are traditional and common approaches. Schemes from these methods are usually designed for image content authentication, which makes trade-off between security and robustness. Robustness means that if the image is edited with benign operations such enhancement and compression, the image can still be verified as valid, but if the image is edited by operations leading to content distortion, the verification will fail. Security means the aforementioned verification is correctly happened with high probability(maybe high than 99%). However, the traditional authentication methods have two disadvantages: (1) The security is not provable and probability of mistake is usually unnegligible; (2) They do not support authorization, which can not provide technical support for some useful image applications such as licensing and assignment of image using rights. As a result, image editing authorization and proof with technical methods is still an open problem.

This paper provides a feasible solution to image editing authorization and proof with cryptographic primitives. To be noticed that, the new design is provable secure. With the new design, image copyright holder can grant rights of image editing operations to specific users. This research is mainly supported by the National Natural Science Foundation of China(61902070), a project which aims to achieve both flexibility and security in image authentication, especially in image editing authentication and authorization, which is the third part of the research contents in the project.