

融合笔迹特征的可信签字图章生成及验证方法

李莉, 高尚, 左珮良, 宣佳铮, 宋涵

(北京电子科技学院, 北京 100070)

摘要: 随着电子通信与互联网技术的迅速发展, 文件流转和处理正在逐步转向数字化, 电子文件的签署方式呈现出更为便捷灵活与多样化的趋势, 如在线签字采集、远程签字确认以及电子签名认证等。与此同时, 文件的签署和验证过程在真实性、完整性等方面面临着诸多严峻挑战。不法分子以低成本手段截取、复制和伪造签字图像冒名签署文件、篡改和伪造签名文件等案例层出不穷, 电子签章系统的应用过程面临成本较高、部署受限、普适性缺乏, 以及真实性和一致性校验复杂等方面的困境。为了应对这些潜在的风险和挑战, 实现个人文件签署流转过程中的可靠验证, 提出了一种融合笔迹特征的可信签字图章生成及验证方法, 该方法主要通过可信身份认证平台的人脸识别和身份信息匹配功能, 融合签字笔迹特征, 对签字笔迹特征唯一绑定并对签名者身份可靠认证, 并基于此生成融合笔迹特征、签署文件验证链接和数字签名二维码的签字图章。分析表明: 所提方法的签字图章不仅具备身份验证的功能, 而且能够实现对文件签署真实性的辨别, 二维码中签署文件验证链接可通过在线渠道直接验证签名人的身份、笔迹以及签署文件的真实性和一致性, 这为纸质文件验证提供了更为便捷的途径, 所提方法在电子文件流转处理和电子与纸质文件真实性验证领域具有广泛的应用前景。

关键词: 笔迹特征; 数字签名; 签字图章; 二维码; 可信签字

中图分类号: TN918

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2024007

Generation and verification method of trusted signature seal incorporating handwriting features

LI Li, GAO Shang, ZUO Peiliang, XUAN Jiazheng, SONG Han

Beijing Electronic Science and Technology Institute, Beijing 100070, China

Abstract: With the rapid development of electronic communication and internet technology, the digitization of document circulation and processing has become increasingly prevalent. The trend towards greater convenience, flexibility, and diversity in electronic document signing is evident through practices such as online signature collec-

收稿日期: 2023-11-13; 修回日期: 2024-01-04

通信作者: 高尚, gaoshangnoble@sina.cn

基金项目: 中央高校基本科研业务费 (328202244, 328202272, 3282023043)

Foundation Item: The Fundamental Research Funds for the Central Universities (328202244, 328202272, 3282023043)

引用格式: 李莉, 高尚, 左珮良, 等. 融合笔迹特征的可信签字图章生成及验证方法[J]. 网络与信息安全学报, 2024, 10(1): 48-57.

Citation Format: LI L, GAO S, ZUO P L, et al. Generation and verification method of trusted signature seal incorporating handwriting features[J]. Chinese Journal of Network and Information Security, 2024, 10(1): 48-57.

tion, remote signature confirmation, and electronic signature authentication. However, the signing and verification processes face challenges related to authenticity, integrity, and more. Instances of unlawful entities intercepting, copying, and forging signature images using low-cost methods to sign documents with false identities, as well as tampering with and forging signature files, are common. The application of electronic signature systems also encounters obstacles such as high costs, limited deployment, lack of universality, and complexities in real-time and consistent verification. To address these risks and challenges and ensure reliable verification in personal document signing processes, a credible method for generating and verifying signature seals that integrate handwriting features was proposed. This method primarily utilized the facial recognition and identity information matching functions of a trusted identity authentication platform. It integrated signature handwriting features and uniquely bound them to the signer's identity for reliable authentication. Accordingly, a signature seal with integrated handwriting features, a verification link for the signed document, and a digital signature QR code were generated. Analysis indicates that the signature seal produced by the proposed method not only serves the purpose of identity verification but also enables the discernment of the authenticity of the signed document. The verification link embedded in the QR code can directly validate the signer's identity, handwriting, and the authenticity and consistency of the signed document through online channels, providing a convenient means for the verification of both electronic and paper documents. The proposed method holds broad application prospects in the fields of electronic document circulation and the verification of the authenticity of electronic and paper documents.

Keywords: handwriting features, digital signature, signature seal, QR code, trustworthy signature

0 引言

在数字化、信息化趋势下,越来越多的文件采用数字化的形式产生、处理、传输及存储,实现了高效、便捷的文件管理^[1-2]。“签字确认”的形式变得丰富,如在线签字采集、远程签字确认和电子签名认证等,其过程变得更加灵活和便利,极大地提高了人们的工作效率,特别是线上办公和远程签字签约,为经济生产的顺利运转提供了重要支持。但不法分子更容易通过截取、复制、伪造签名等低成本手段完成文件的冒名签署,仅使用“笔迹特征”这一重要生物特征验证签名人身份已缺乏可靠性。因此,基于签字笔迹特征,生成可对签名人身份和被签署文件进行一致性校验的签字图章就显得十分重要。

近年来,为了确保文件签署的可信性,电子签章技术得到了广泛应用。在政府、高校以及其他企事业单位的信息化建设过程中,基于公钥基础设施(PKI, public key infrastructure)技术的电子签章在一定程度上保障了公文流转系统内文件的可靠签署和验证。与此同时,许多签名软件应运而生,为用户签署文件提供了便利。这些措施提高了文件处理效率,具备较高的安全保障,能

防止冒名签署和伪造行为。然而在实际应用中,电子签章的研究仍面临以下问题。

1) 应用范围受限。电子签章的应用受到两方面的限制,首先,如文献[3-5]提出的基于公钥基础设施的电子印章系统,对文件的格式和验证环境限制较高,且当带有电子签名的文件转存为其他文件形式时验证功能可能缺失;其次,电子签章签名用户局限于特定范围,如高校电子签章系统^[6-7],涉密单位、气象单位^[8-9]等仅适用于本单位的签章系统。此类签章系统签名人基于所在单位身份属性注册账号或持有密钥,文件签署依赖签名人特定网络环境,无法保障跨工作域的可靠签署和验证。

2) 缺乏对签名人的认证。目前签章系统通过证书授权(CA, certificate authority)机构对签名设备或者账号进行验证,但缺乏对操作签名设备或账号用户的验证。存在他人冒名注册获取签名人账号、伪造或盗用签名签字数据进行冒名签署的风险。同时,存在签名人本人在签署完成后抵赖非本人签署的可能性。

3) 呈现形式单一,效果不直观。多数电子签章以公章图像的形式呈现,如文献[10-11],有些为便于文件跨形式验证,在文档中放置验证二维

码^[12]。然而,对于签字图像的使用较少,这导致电子签章运用于个人文件签署缺乏直观性。

4) 缺乏绑定关系认证。目前已有使用签字笔迹特征进行签名人身份认证的方法^[13],但缺乏对签字图像所在文档的绑定认证。这导致签字图像一旦被盗用,只能确认签字图像是真实的,而无法验证与所签署文档的关联关系。

为解决上述问题,本文提出一种融合签字笔迹特征的可信签字图章生成及验证方法,将认证后的签名人的身份标识和签字图像中的笔迹特征唯一绑定,并生成融合被签署文件验证链接和数字签名的二维码,由签字图像和该二维码结合生成的签字图章进行文件签署,最后通过扫描签字图章完成签名人身份验证和签署文件一致性鉴别。

1 相关理论

本文提出的融合签字笔迹特征的可信签字图章生成及验证方法的重点是将签字图像中的签字笔迹特征和签名人身份标识绑定,并通过此标识完成数字签名验证。因此,正确提取、匹配签字笔迹特征并通过身份标识相关信息进行数字签名和验证是本文方法实现的前提条件。

1.1 SM9 标识密码体制

SM9 是一种基于双线性对的身份认证密码体制^[14],主要用于数字签名、密钥协商和身份认证。相较于基于大数因子分解或离散对数的 RSA 和 DSA 等签名算法,SM9 的安全性更高^[15],且不需要证书,用户的身份标识信息即其公钥,简化了证书管理的烦琐过程。

SM9 的工作流程主要包括系统初始化、密钥提取、签名生成和签名验证 4 个步骤。在系统初始化阶段,选择一对双线性对,生成系统的主公钥和主私钥。在密钥提取阶段,使用系统的主私钥和用户的身份标识信息,生成用户的签名密钥。在签名生成阶段,用户使用自己的签名密钥和待签名的消息,生成数字签名。在签名验证阶段,任何人都可以使用系统的主公钥、用户的身份标识信息、待验证的消息和数字签名,来验证签名的有效性。

1.2 签字笔迹特征

笔迹特征通常以描述符的形式表示,描述符

是从图像中提取的角点、边缘等关键点的数值化表示。描述符可用于各种计算机视觉任务,如图像的视觉内容比较、图像匹配、对象识别和图像检索,以及加强图像信息与计算机视觉的模式重建与匹配程度等^[16]。

常用的签字笔迹特征描述符包括尺度不变特征转换(SIFT, scale-invariant feature transform)、加速鲁棒特征(SURF, speeded up robust features)和 ORB(oriented FAST and rotated BRIEF)等。这些描述符可以捕捉到签字笔迹的形状、纹理、方向等特征。通过比较不同签字笔迹的描述符,可以进行签字笔迹的匹配和识别。常用的匹配算法包括暴力匹配^[17]和快速近似最近邻(FLANN, fast library for approximate nearest neighbors)搜索匹配^[18]等。

2 签字图章生成及验证方法

2.1 总体思路

考虑到签字笔迹与签名者和被签署文件的关联关系,并结合二维码技术的普遍和便捷应用这一现实情况,本文方法拟将签字图像中笔迹的特征值与签名人身份信息绑定,并将签名人签署操作的相关信息进行二维码编码后与签字图像相结合生成签字图章,验证时通过扫描签字图章中的二维码和签字图像完成文档签署一致性校验。此过程依托互联网+可信身份认证平台(CTID),进而实现可信签字图章生成和验证,对应场景如图 1 所示,包括 5 个实体。

签名人(SW, sign writer):使用邮箱、身份证件关键信息、人脸数据和签字图像完成账号注册和身份认证,操作签章生成。

验证方(VS, validation staff):扫描签章二维码和签字图像,完成签名人身份验证和签署文件一致性校验。

云平台(CP, cloud platform):绑定并存储签名人签字笔迹特征和身份标识信息;备案签署文档影像;接收验证方验证请求,进行验证并反馈验证结果。

密钥生成中心(KGC, key generation center):根据签名人的身份标识 ID 采用 SM9 标识密码算法生成签名密钥 D_{ID} 。

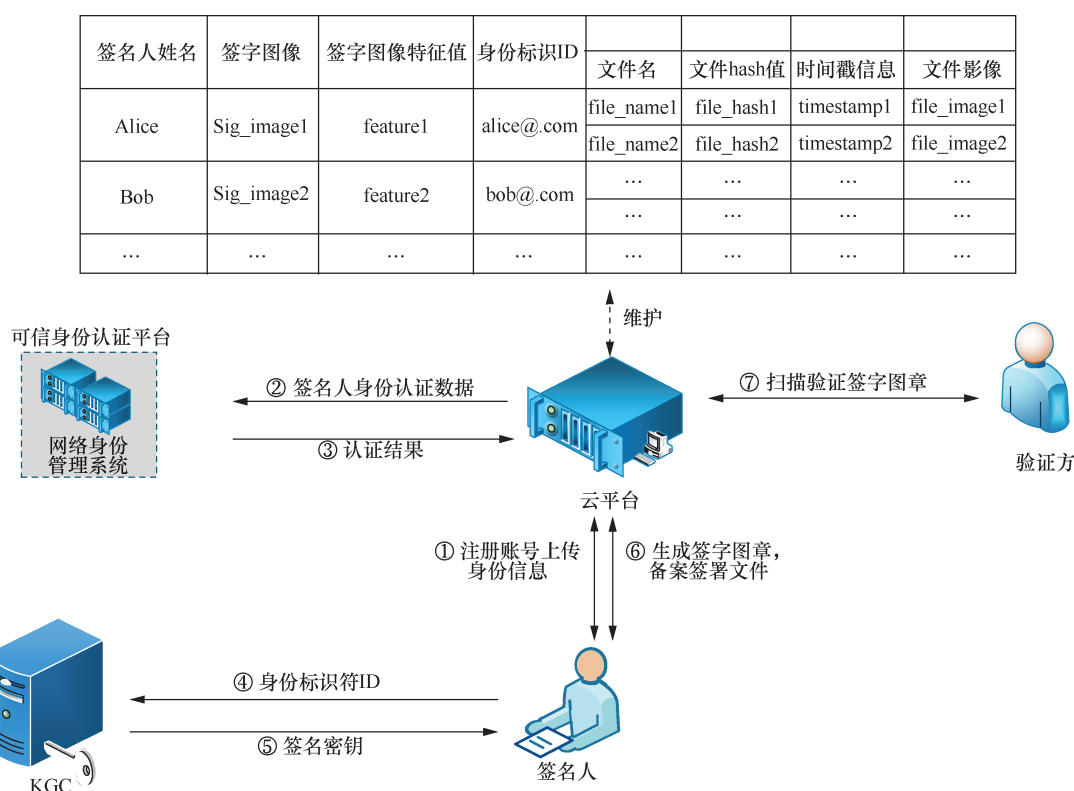


图 1 可信签字图章生成和验证场景
Figure 1 Trustworthy signature seal generation and verification scenario

可信身份认证平台：中华人民共和国公安部第一研究所可信身份认证平台是一种基于区块链技术的身份认证系统。以居民身份证制证数据为基础，以人脸识别为生物技术，对外提供真实身份核验、网证开通和管理、网证认证三大功能。在本文方法中，CTID 通过签名人身份证件信息和人脸信息完成对签名人的认证。

2.2 签名人身份注册

由于签字图章生成和使用过程与签名人的身份信息直接相关，因此需要在首次使用时对签名人身份进行注册并认证。签名人身份注册流程如图 2 所示。

1) 签名人使用邮箱申请用户账号，并上传本人的有效身份证信息，通过可信身份认证平台进行人脸识别和身份信息匹配认证，可信身份认证平台向云平台反馈认证结果。

2) 签名人将申请账号时使用的邮箱作为身份标识 ID 上传至 KGC，此 ID 即签名人的公钥。KGC 根据 ID 使用 SM9 标识密码算法生成签名密钥 D_{ID} 并通过安全通道反馈给签名人。

3) 签名人在云平台内上传签字图像，为防止用户使用他人已注册的签字图像恶意注册，云平台提取签字图像中的笔迹特征并在系统内进行唯一性校验，以判断该签字图像是否已被注册登记。若通过校验，则将签字图像特征值、签名人身份信息和身份标识 ID 进行唯一绑定，完成签名人身份注册；若未能通过校验，则直接拒绝签名人的注册请求。

2.3 签字图像笔迹特征提取及匹配

签字图像笔迹特征提取使用开源的 OpenCV 库，通过预处理、关键点提取和描述符计算等步骤实现，具体流程如图 3 所示。

1) 图像预处理：将签字图像灰度图通过 noiseRemoval 函数降噪后转换为黑白两色的二值图像；利用 strokeSeg 函数将笔迹从背景中分离出来，获得正规化图像 normim 和笔迹掩码 mask，利用 strokeOrient 和 strokeFreq 函数分别计算 normim 中的笔迹方向 orient 以及笔迹密度和方向变化频率，取平均值后与 mask 相乘，得到最终的笔迹频率 freq；再将正规化图像 normim、笔迹

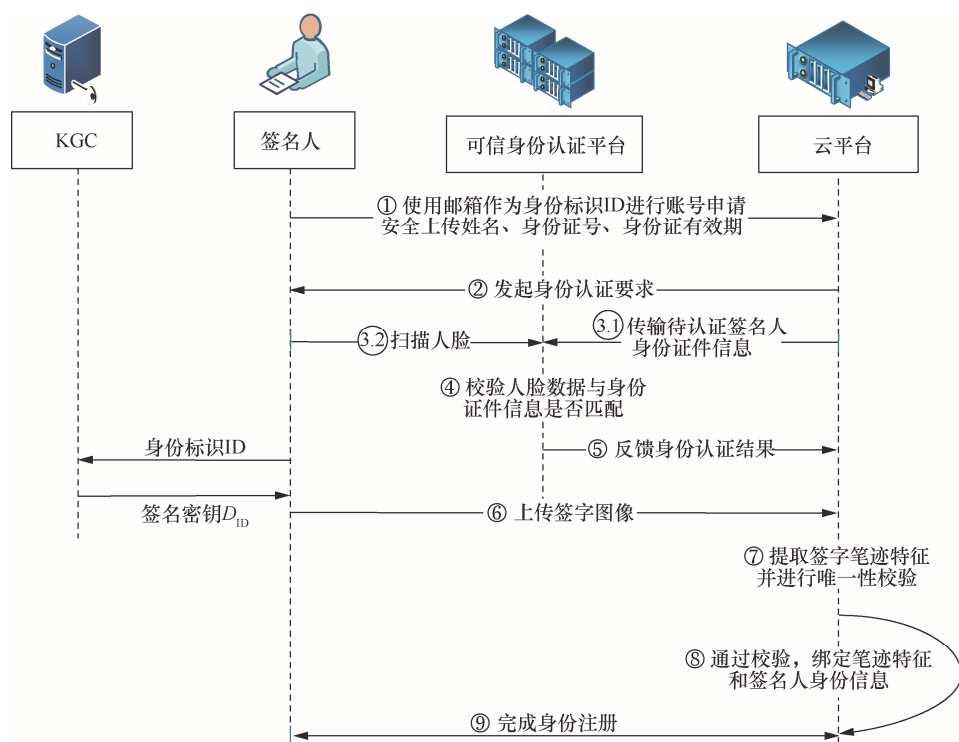


图2 签名人身份注册流程

Figure 2 Signature party identity registration process

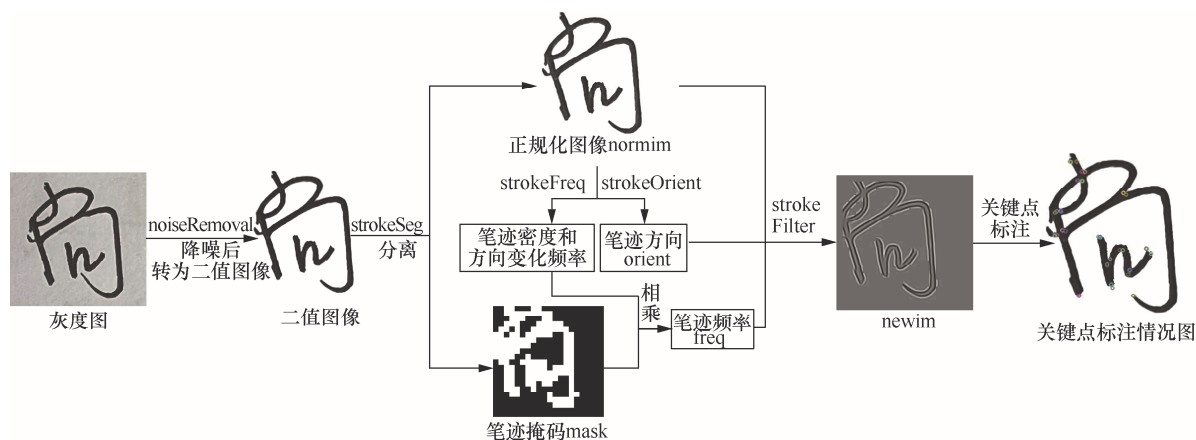


图3 签字图像笔迹特征提取流程

Figure 3 Signature image handwriting feature extraction process

方向 orient 和笔迹频率 freq 作为输入, 去除图像中的噪声, 生成新图像 newim。

2) 关键点提取: 角点指图像中一些突然变化或弯曲的点, 它们所在区域的灰度值在多个方向上都有显著变化, 可以用来表示签字图像中的特征。这里采用 cornerHarris 角点检测算法获取签字图像笔迹中的角点, 并通过阈值筛选掉结果中的

噪声后, 将其作为关键点进行标注。

3) 描述符计算: 使用 ORB 算法计算关键点的方向、尺度等特征, 并将这些特征以 NumPy 数组的格式存储, 作为关键点的描述符。

笔迹特征描述符匹配的过程使用暴力匹配器, 其工作原理为计算被验证图像的每个关键点描述符与参考图像中的所有关键点描述符之

间的汉明距离，选择汉明距离最小的参考图像关键点描述符作为匹配。在被验证图像的所有关键点描述符都匹配完成后，计算这些匹配汉明距离的平均值，并与预设的阈值相比较，若小于该阈值，则判定两幅签字图像为同一人的签字笔迹。描述符匹配结果的图形化示例如图4所示。



图4 描述符匹配结果的图形化示例
Figure 4 Example of graphical descriptor matching results

2.4 签字图章生成

签字图章生成流程可以分为文档信息二维码的生成和与签字图像组合两部分，如图5所示。

1) 签名人发起签名操作，明确待签署文件信息 M ，计算明文摘要 $M_{\text{hash}} = \text{SM3}_{\text{hash}}(M)$ ，使用签名密钥 D_{ID} 对 M_{hash} 签名得到签名结果 $(M_{\text{kdf}}, S) = \text{SM9}_{\text{sign}}(D_{\text{ID}}, M_{\text{hash}})$ ，并将 $N = \text{ID} || M_{\text{hash}} || (M_{\text{kdf}}, S)$ 发送给云平台。

2) 云平台对数据 N 进行数字签名得到签名值 $S_N = \text{Sign}(\text{sk}_{\text{云平台}}, N)$ 。随后将数据 N 、数字签名 S_N 以及使用了超文本传输安全协议 (HTTPS) 的云平台签名验证访问端口统一资源定位符 (URL) 生成二维码，将该二维码与签字图像组合，生成签字图章。

云平台将签字图章反馈给签名人，签名人使用签字图章完成文件签署后将签署文件影像上传至云平台进行登记，此时签字图章生效。

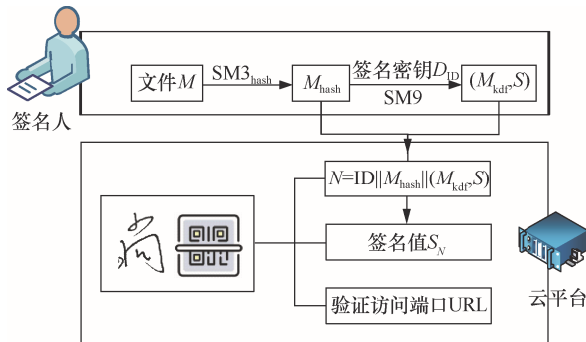


图5 签字图章生成流程
Figure 5 Signature seal generation process

2.5 签字图章验证

签字图章验证流程分为二维码信息验证提取、签字特征提取和签署一致性校验，如图6所示。

1) 验证方进行签字图章验证时，可通过带有二维码扫描功能的手机软件扫描签字图章中的二维码，获取云平台签名验证访问端口 URL、数据 N 和签名值 S_N 。

2) 验证方通过 HTTPS 验证云平台签名验证访问端口 URL 的合法性后与其建立安全连接。从该 URL 的数字证书中获取云平台的公钥从而对签名值 S_N 进行验签操作，若未能通过签名验证，则证明签字图章被篡改，签章无效。

3) 验证方扫描签字图章中的签字图像，提取其笔迹特征，连同二维码中获取的身份标识 ID 一并上传至云平台，在云平台内将提取出的笔迹特征与签名人签署文件登记表中该身份标识 ID 所对应的签名人的笔迹特征进行比较。若通过匹配验证，则证明该签字图像和二维码是对应的；若未通过匹配，则证明该签章中签字图像已被篡改，签字图章失效；若签署文件登记表找不到该身份标识 ID 对应的笔迹特征信息，则证明该身份标识 ID 对应的签名人未在平台内注册过身份，签章是无效的。

4) 验证方根据签名人身份标识 ID 计算验签密钥 Q_{ID} ，通过 SM9 标识密码算法进行计算得到 $M'_{\text{kdf}} = \text{SM9}(M_{\text{hash}}, Q_{\text{ID}}, S)$ 。

5) 对比二维码中 M_{kdf} 和计算结果 M'_{kdf} ，若两者不同，则说明签字图章中签字图像所对应签名人身份信息与二维码所属签名人身份信息不符，签字图章为伪造图章；若两者相同，则在云平台签字图像特征所对应的签署列表内检索签署文件，并将该签署文件影像和签名人身份信息反馈给验证方。

6) 验证方对比所持文件与云平台反馈文件内容是否一致，若一致则证明签字图章有效，若不一致则证明该签章签署文件已被篡改或该签章被盗用至当前文件，文件签署无效。

3 安全性分析

签字图章在应用过程中可能面临如下风险。

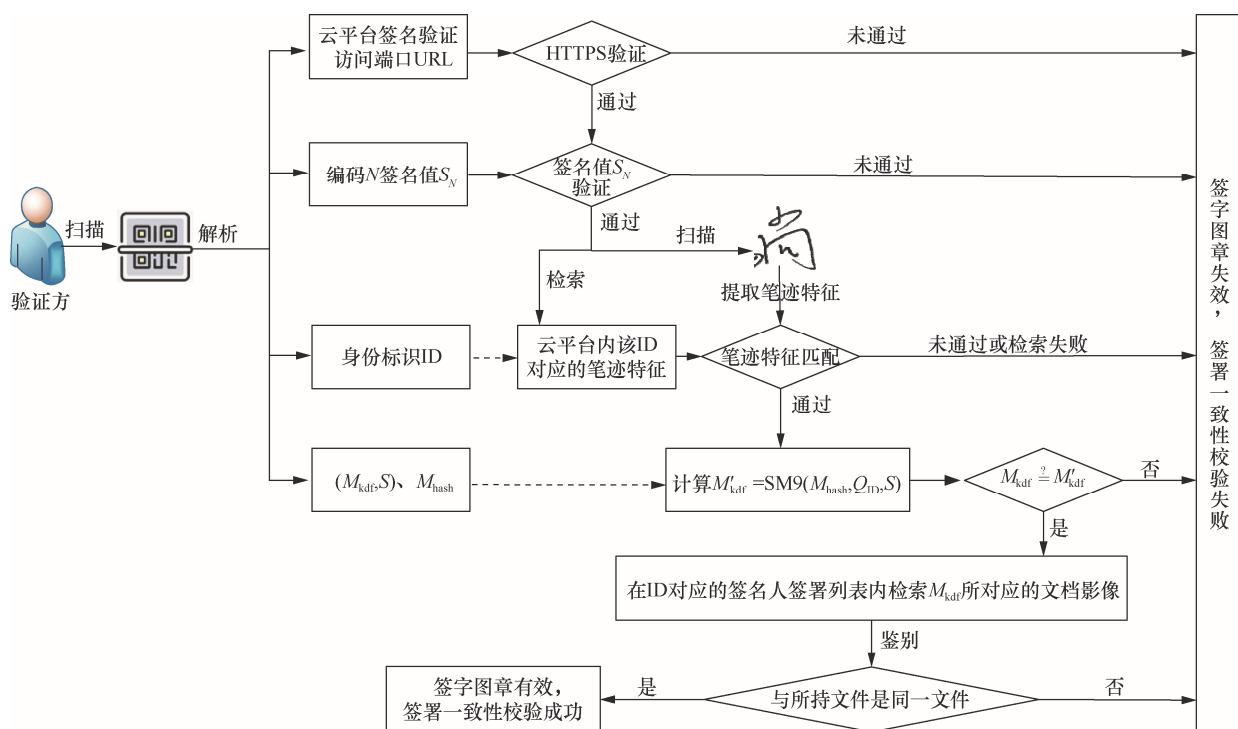


图 6 签字图章验证流程

Figure 6 Signature seal verification process

1) 冒名注册: 攻击者使用签名人身份证件信息冒名注册账号、使用他人签字图像登记身份、截取已注册用户的签字图像登记身份。

2) 签名人抵赖: 签名人谎称签章生成数据被盗用从而抵赖生成实际有效的签字图章。

3) 签字仿冒: 攻击者仿写或截取签名人签字。

4) 二维码篡改: 攻击者篡改签字图章中的二维码内容。

5) 签署文档篡改: 签字图章签署的文件被篡改。

6) 文件形式变化: 已签署文件格式、形态、所处环境等发生变化。

针对如上 6 种签字图章生成及验证过程中存在的风险, 本文所提方法具有如下安全性。

3.1 抗冒名注册

本文方法在注册阶段使用中华人民共和国公安部第一研究所“互联网+可信身份认证平台”网络身份管理系统真实身份核验平台, 以居民身份证制证数据为基础, 以人脸识别为生物技术手段, 以权威可信的数据对比信息源, 保证注册人身份信息和身份认证结果的准确可靠, 有效防止攻击者通过

获取他人身份证件信息进行冒名注册的过程。

同时, 本人注册后, 签字图像仅可上传一次, 且与身份信息进行唯一绑定, 验证时云平台会向验证方反馈签名人身份注册时的姓名等身份信息, 因此若攻击者注册时使用他人签字图像, 则在验证时将产生反馈的签名人信息和签字图像内容不符的现象; 若签名人注册时使用的是他人已经注册过的签字图像, 则系统将直接拒绝注册请求, 抵抗违规注册的风险。

3.2 抗签名人抵赖

本文提出的签章生成方法在签名人生成签章前, 需要通过人脸识别进行身份认证, 确保签章生成操作由本人授权完成, 既可以防止攻击者使用签名人设备或账号冒名生成签章, 也可以有效防止签名人签署文件后谎称签名数据被盗用而不承认签署有效性的问题。

3.3 抗签字仿冒

在本文方法中, 签字笔迹的特征与签名人身份信息唯一绑定且与签名人签署文档绑定, 验证时平台会根据签名人身份标识 ID 定位对应的签字图像特征, 并与验证方上传的签字图像特征进

行匹配。因此,若攻击者仿冒签名人签字,则会在笔迹特征匹配验证时失败,平台会向验证方反馈签字图章验证失败的结果。即使攻击者伪造的签字通过了笔迹特征匹配验证,验证方仍可通过后续对二维码的验证完成签字图章签署一致性校验。

3.4 抗二维码篡改

本文生成的签字图章中的二维码会经过两部分验证,首先对其中所含的“云平台签名验证访问端口 URL”,通过 HTTPS 对其数字证书进行验证,若认证失败,则证明 URL 被篡改,二维码无效;之后从数字证书中获取公钥对数据 N 和其签名值 S_N 进行验证,若验签失败,则说明编码内容或签名被篡改,二维码无效;若攻击者将非同一人的有效签字图像和有效文档二维码拆分重组使用,则会因签字图像匹配不成功而验证失败。

3.5 抗签署文档篡改

若攻击者将有效签字图章(含签名图片和签署文档信息二维码)直接挪用在其他文档中或将已签署文档进行篡改,在进行签字图章验证时,会在签字图章验证本身验证有效后向用户反馈该有效签字图章在系统内备案的签署文档影像信息,验证者可将手持文件与系统反馈文档影像信息进行对比,完成签署一致性校验。

3.6 抗文件形式变化

本文提出的可信签字图章验证主要通过二维码和签字图像扫描完成,不受被验证文件的格式、呈现载体形式和所处环境限制,因此在绝大多数情况下可完成签字图章验证。

4 方法实现与功能验证

融合签字笔迹特征的可信签字图章生成和验证系统采用“ZION 无代码开发平台”实现,身份信息认证和核验使用 CTID 易捷开放平台提供的标准化的 API 接口,通过“四项信息+人像”即姓名、身份证号码、身份证有效期起止日期和人像完成一致性对比。签章生成验证主要界面如图 7 所示。

图 7(a)为可信签字图章生成及验证小程序首页,签名人可点击“签名人注册”,使用邮箱进行

账号申请,申请成功后跳转至图 7(b)所示的身份认证界面,使用身份证“四项信息”和人像进行身份信息认证。注册成功后即可根据文件信息生成签字图章,并完成文件签署,签署界面如图 7(c)所示,验证时会反馈签章验证成功与否,若成功则显示图 7(d)所示的界面,若失败则显示图 7(e)所示的界面。



图 7 签章生成验证主要界面

Figure 7 The main interface for generating signatures

5 结束语

本文针对签字图像存在可以使用低成本手段截取、复制和伪造后用于文件冒名签署的问题,提出了一种融合笔迹特征的可信签字图章生成及验证方法。在该方法中,签名人身份和签字笔迹特征在云平台内被唯一绑定,签名人使用与自己身份标识信息相关联的签名密钥对文件进行数字签名,并将签署过程中产生的相关数据上传至云平台。云平台对这些数据进行签名后和验证访问链接一起编码成二维码,并

将该二维码和签名人签字图像进行结合,生成签字图章,以实现对签名人和被签署文件的签署一致性校验。

验证过程中验证方分别对验证平台、二维码内容、签字笔迹和被签署文件进行真伪校验,最终完成签字图章的可信验证。验证结果表明,所提方法能够完成签字图章的可信生成与验证,可抵抗签字图像被截取盗用后冒名签署文件的风险,能够在文件电子签署领域得到良好应用。

参考文献:

- [1] 巴志超, 刘学太, 马亚雪, 等. 国家安全大数据综合信息集成的战略思考与路径选择[J]. 情报学报, 2021, 40(11): 1139-1149.
BA Z C, LIU X T, MA Y X, et al. Strategic thinking and path selection of information integration of big data for national security[J]. Journal of the China Society for Scientific and Technical Information, 2021, 40(11): 1139-1149.
- [2] 金波, 杨鹏, 添志鹏, 等. 大数据时代档案数据生态平衡与调适[J]. 图书情报知识, 2023, 40(1): 13-22.
JIN B, YANG P, TIAN Z P, et al. Balance and adjustment of archival data ecologies in big data era[J]. Documentation, Information & Knowledge, 2023, 40(1): 13-22.
- [3] ZHAO X F. Design of electronic seal system based on PKI[C]//Proceedings of the 2011 International Conference on E-Business and E-Government (ICEE). 2011: 1-3.
- [4] BIN M, JIAN X. Electronic seal system based on RSA algorithm and public-key infrastructure[C]//Proceedings of the 2010 International Conference on Networking and Digital Society. 2010: 636-639.
- [5] YU Y C, HOU T W, CHIANG T C. Dual function seal: visualized digital signature for electronic medical record systems[J]. Journal of Medical Systems, 2012, 36(5): 3115-3121.
- [6] 钟梅, 董茜, 徐旭光, 等. 高校可信电子证明材料实现方法研究: 以电子成绩单为例[J]. 信息系统工程, 2023(1): 137-139.
ZHONG M, DONG Q, XU X G, et al. Research on the realization method of trusted electronic proof materials in colleges and universities—taking electronic transcripts as an example[J]. China CIO News, 2023(1): 137-139.
- [7] 刘淑云, 胡美琴, 王文君, 等. 基于资产平台的设备维修合同电子签章系统的设计与实现[J]. 实验室研究与探索, 2021, 40(11): 272-276.
LIU S Y, HU M Q, WANG W J, et al. Design and implementation of equipment maintenance contract electronic signature system based on asset platform[J]. Research and Exploration in Laboratory, 2021, 40(11): 272-276.
- [8] 杨姣璇. 面向涉密单位的电子签署系统开发[D]. 绵阳: 西南科技大学, 2020.
YANG J L. Development of electronic signature system for secret-related units[D]. Mianyang: Southwest University of Science and Technology, 2020.
- [9] 王甫棣, 王帅, 汪芳. 气象部门国产化电子签章云服务的设计与实现[J]. 气象科技, 2021, 49(5): 716-722.
WANG F D, WANG S, WANG F. Design and implementation of China meteorological administration E-signature cloud service in nationalization environment[J]. Meteorological Science and Technology, 2021, 49(5): 716-722.
- [10] LIU G Y, LI J Y. An algorithm of extracting signature and seal of electric power marketing inspection documents[C]//Proceedings of the 2022 IEEE 6th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC). 2022: 967-970.
- [11] CHEN Y Y, LIU Y Q, ZHUANG L, et al. Application research of electronic authorized steganographic seal management and control platform based on invisible watermark[C]//Proceedings of the 2021 International Conference on Management Science and Software Engineering (ICMSSE). 2021: 253-256.
- [12] LIU X M, TANG X. Image authentication using QR code watermarking approach based on image segmentation[C]//Proceedings of the 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications(TrustCom). 2020: 1572-1577.
- [13] VINOD B, SENTHIL KUMAR A M. Handwritten signature identification and fraud detection using deep learning and computer vision[C]//Proceedings of the 2023 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS). 2023: 196-200.
- [14] 赖建昌, 黄欣沂, 何德彪, 等. 基于商密 SM9 的高效标识签密[J]. 密码学报, 2021, 8(2): 314-329.
LAI J C, HUANG X Y, HE D B, et al. An efficient identity-based signcryption scheme based on SM9[J]. Journal of Cryptologic Research, 2021, 8(2): 314-329.
- [15] 赖建昌, 黄欣沂, 何德彪, 等. 国密 SM9 数字签名和密钥封装算法的安全性分析[J]. 中国科学: 信息科学, 2021, 51(11): 1900-1913.
LAI J C, HUANG X Y, HE D B, et al. Security analysis of SM9 digital signature and key encapsulation[J]. Scientia Sinica (Informationis), 2021, 51(11): 1900-1913.
- [16] PARVAIZ A, KHALID M A, ZAFAR R, et al. Vision transformers in medical computer vision—a contemplative retrospection[J]. Engineering Applications of Artificial Intelligence, 2023, 122: 106126.
- [17] 廖泓真, 王亮, 孙宏伟, 等. 一种改进的 ORB 特征匹配算法[J]. 北京航空航天大学学报, 2021, 47(10): 2149-2154.

LIAO H Z, WANG L, SUN H W, et al. An improved ORB feature matching algorithm[J]. Journal of Beijing University of Aeronautics and Astronautics, 2021, 47(10): 2149-2154.

- [18] WANG B Y, ZHANG X H, WANG W B. Feature matching method based on SURF and fast library for approximate nearest neighbor search[J]. Integrated Ferroelectrics, 2021, 218(1): 147-154.

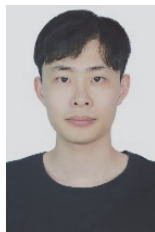
[作者简介]



李莉（1974—），女，山东青岛人，北京电子科技学院教授，主要研究方向为网络与系统安全、嵌入式安全。



左珮良（1991—），男，山东烟台人，北京电子科技学院讲师，主要研究方向为物联网、网络安全与防御、电子公文。



宣佳铮（1998—），男，浙江绍兴人，北京电子科技学院硕士生，主要研究方向为信息安全、密码学。



高尚（1999—），男，山西临汾人，北京电子科技学院硕士生，主要研究方向为信息安全、密码学。



宋涵（2000—），男，山东菏泽人，北京电子科技学院硕士生，主要研究方向为人工智能、嵌入式安全。