一种可隐藏敏感文档和发送者身份的区块链隐蔽通信模型

佘 维[1,2,3],霍丽娟[1,2],刘 炜[1,2,3],张志鸿[2,4],宋 轩[1,2],田 钊[1,2]
(1. 郑州大学网络空间安全学院,河南郑州 450000; 2. 郑州市区块链与数据智能重点实验室,河南郑州 450000;
3. 河南省互联网医疗卫生服务协同创新中心,河南郑州 450000; 4. 郑州大学信息工程学院,河南郑州 450000)

摘 要: 目前,区块链隐蔽通信的研究主要是通过发起多笔交易来传输一条短消息,这一方式不仅不适用于敏感数据量大的情况,还可能存在有些交易没有被打包而造成秘密信息的丢失,而且传输过程没有隐藏发送方身份. 部分区块链隐蔽通信的研究中使用的图像隐写术虽然具有嵌入率高这一优点,但是越来越难以抵御基于统计特征的检测分析. 针对以上问题,本文提出一种可隐藏敏感文档和发送者身份的区块链隐蔽通信模型. 首先发送方使用密文策略的属性基加密(Ciphertext-Policy Attribute-Based Encryption,CP-ABE)对敏感文档进行加密,得到加密文档后将其上传至星际文件系统(Inter Planetary File System,IPFS);然后发送方利用基于生成式对抗网络(Generative Adversarial Networks,GAN)的图像隐写术将加密文档的哈希值嵌入载体图像中,得到载密图像后将其上传至IPFS;接着发送方创建一笔含有载密图像的哈希值的交易,交易经环签名之后广播到区块链网络中进行验证打包上链;之后,接收方从交易中读取载密图像的哈希值并通过上述步骤的逆过程得到加密文档;最后接收方根据CP-ABE设置的访问控制策略解密加密文档得到敏感文档. 实验结果表明,该模型在传输秘密信息量上从KB提升至MB,而且具有较高的隐蔽性和安全性.

关键词: 区块链; 隐蔽通信; 基于生成式对抗网络的图像隐写术; 环签名; 密文策略的属性基加密; 星际文件系统

中图分类号: TP309.2 **文献标识码:** A **文章编号:** 0372-2112(2022)04-1002-12

电子学报URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20211021

A Blockchain-Based Covert Communication Model for Hiding Sensitive Documents And Sender Identity

SHE Wei[1,2,3],HUO Li-juan[1,2],LIU Wei[1,2,3],ZHANG Zhi-hong[2,4],SONG Xuan[1,2],TIAN Zhao[1,2]
(1. *School of Cyber Science and Engineering, Zhengzhou University, Zhengzhou, Henan* 450000 *China*;
2. *Zhengzhou Key Laboratory of Blockchain and Data Intelligence, Zhengzhou, Henan* 450000 *China*;
3. *Henan Collaborative Innovation Center for Internet Medical and Health Services, Zhengzhou University, Zhengzhou, Henan* 450000, *China*;
4. *School of Information Engineering, Zhengzhou University, Zhengzhou Henan* 450000 *China*)

Abstract: At present, the research of blockchain covert communication mainly transmits a short message by initiating multiple transactions. This method is not suitable for situations where there is a large amount of sensitive data. And there may be some transactions that are not packaged, resulting in loss of secret information. Meanwhile, the sender´s identity is not hidden during the transmission. Although the traditional image steganography used in some research has the advantage of high embedding rate, it is increasingly difficult to resist detection and analysis based on statistical features. To solve the above problems, this paper proposes a blockchain-based covert communication model for hiding sensitive documents and sender identity. First, the sender encrypts a sensitive document using cipertext-policy attribute-based encryption(CP-ABE), and then uploads the encrypted document to inter planetary file system(IPFS). Next, the sender embeds the hash value of the encrypted document into a cover-image employing the image steganography based on generative adversarial net-

收稿日期:2021-08-01;修回日期:2022-03-13;责任编辑:崔兴华
基金项目:河南省高校科技创新人才支持计划(No.21HASTIT031);河南省重大公益专项(No.201300210300);河南省重点研发与推广专项(No.212102310039,212102310554);郑州大学教育教学改革研究与实践项目(No.2021ZZUJGLX168)

works(GAN), and then uploads the stego-image to IPFS. After that, the sender creates a transaction containing the hash value of the stego-image and signs it using the ring signature, and then broadcasts the transaction to the blockchain network for verification and package into a block. Then the receiver reads the hash value of the stego-image from the transaction and obtains the encrypted document through the inverse process of the above steps. Finally, the receiver decrypts the encrypted document and obtains the sensitive document according to the access control policy set by CP-ABE. The experimental results show that the model can greatly improve the capacity of secret information from KB to MB during the transmission, and has high concealment and security.

Key words: blockchain; cover communication; image steganography based on generative adversarial networks (GAN); ring signature; cipertext-policy attribute-based encryption(CP-ABE); inter planetary file system(IPFS)

1 前言

传统的隐蔽通信是将秘密信息隐藏于常用的载体中进行隐蔽传输的技术[1],在信息安全、数据通信等方面发挥着重要作用. 常用的载体包括图像、文本、音频、视频等,其中图像因其具有较高的有效载荷能力,是广泛使用的载体格式[2]. 但是在传统的隐蔽通信过程中,载体信息可能会面临被删除或者篡改的风险,从而导致嵌入的秘密信息被破坏. 而且在此过程中,通信双方的身份暴露在网络中,攻击者可以对通信进行针对性的干扰和阻断.

相比于其他的通信媒介,区块链具有抗篡改、防伪造、匿名性等特点[3~5]. 抗篡改使得隐蔽通信的攻击者对秘密信息的删除和篡改都是无效的;防伪造使得隐蔽通信的攻击者不能伪造秘密信息的内容;匿名性使得隐蔽通信的双方可以进行匿名通信,不必暴露真实身份. 因此,一些研究使用区块链作为通信媒介来解决传统隐蔽通信面临的问题. Partala等人[6]首次提出了将秘密信息嵌入区块链交易地址的最低位进行隐蔽传输,并对其安全性进行了研究和验证. Akbari等人[7]利用基于区块链的交易隐写术和图像隐写术实现了一种安全机密的通信方式. Liu等人[8]将区块链交易数据的敏感部分加密隐藏到HEVC视频中,以保护区块链的隐私交易数据. She等人[9]将区块链和星际文件系统(Inter Planetary File System,IPFS)结合实现一种双重隐写术,并解决大文件的载密载体在区块链中的存储问题. 这些研究都是对一条短消息进行隐蔽传输. 但是随着区块链在智慧城市、智慧医疗、智慧政务等领域的大量应用和飞速发展,需要进行隐蔽通信的数据量越来越大,短消息的隐蔽传输并不适用于敏感数据量大的情况. 而且上述区块链隐蔽通信的研究中主要还存在以下尚未解决的问题.

(1)都未隐藏发送方身份,存在发送方身份泄露问题,增加了隐蔽信道暴露的风险.

(2)都难以对数据量大的MB级敏感数据进行隐蔽传输.

(3)都需要从发送方发起大量的交易来嵌入秘密信息,它们的统计特性容易引起攻击者察觉,且耗时较长,还存在某些交易未被打包而造成信息缺失的缺点.

(4)一些研究中采用的图像隐写术都是以一般的图像作为载体,载体图像经过嵌入秘密信息得到载密图像,在这一过程中,载体图像的修改痕迹会比较大. 随着隐写分析技术的发展,以一般的图像作为载体的隐写术越来越难以抵抗基于统计特征的检测分析.

基于以上问题,本文提出一种可隐藏敏感文档和发送者身份的区块链隐蔽通信模型:H-SD&SI. 首先发送方将敏感文档进行密文策略的属性基加密[10](Ciphertext-Policy Attribute-Based Encryption,CP-ABE),得到加密文档后,将其存储于IPFS,并使用基于生成式对抗网络(Generative Adversarial Networks,GAN)的图像隐写术[11~15]将加密文档的哈希值嵌入由GAN生成的载体图像中,得到载密图像. 发送方发起一笔交易,携带载密图像的哈希值,经过环签名[16]后将交易发布到区块链网络中,最终各节点达到同步状态[17]. 接收方提取本地的交易中携带的载密图像的哈希值,并通过上述方法的逆过程从IPFS中搜索并下载加密文档. 由于使用了CP-ABE的访问控制策略,只有特定的接收方能解密加密文档并获得敏感文档.

本文的主要贡献包括4个方面.

(1)本文首次在区块链隐蔽通信模型中引入环签名来隐藏隐蔽通信的发送方身份,解决了先前基于区块链的隐蔽通信方案都存在的发送方身份泄露问题. 发送方使用自己的私钥和环签名成员的公钥对含有秘密信息的交易进行签名,将自己的身份隐藏起来,有效地保护用户身份隐私,减少了隐蔽信道暴露的风险,提高了通信的隐蔽性,解决了前述问题(1).

(2)本文在区块链隐蔽通信中实现了传输MB级敏感数据. 在隐蔽传输之前,为了提高敏感文档的安全性,发送方利用CP-ABE对敏感文档进行加密. 发送方使用设置的访问策略对敏感文档进行加密并为接收方制定专门的访问策略,接收方利用自己的属性集进行解密. 这一过程不仅避免了密钥的传输,还可以让接收

方不依赖其他附加信息而是利用自己的属性集进行解密. 在加密之后,发送方仅需要对加密文档进行隐写嵌入操作,而不必将相关的密钥同加密文档一起进行嵌入,减少了嵌入量. 较之以往对短消息的隐蔽传输,该方法在保证敏感文档安全性的同时在传输数量级上有较大提高,实现了大量敏感数据的隐蔽传输,解决了前述问题(2).

(3)本文通过使用两次IPFS系统实现只发起一笔交易来传递敏感文档. 第一次是将加密文档上传至IPFS,IPFS返回一串较短的哈希字符串,便于嵌入载体图像生成载密图像;第二次是将载密图像上传到IPFS,IPFS返回一串较短的哈希字符串,便于发送方只发起一笔交易携带此哈希字符串进行隐蔽传输,也避免了区块链直接存储载密图像而造成的存储开销过大的问题. 较之以往发送方发起大量交易来传输秘密信息的方式,本文只发起一笔交易的方式不易引发网络数据非正常事件分析程序的注意,避免引起攻击者察觉,且耗时短,解决了前述问题(3).

(4)本文首次将基于GAN的图像隐写术引入区块链隐蔽通信模型中,以抵抗基于统计特征的检测分析. 本文利用基于GAN的图像隐写术生成符合自然图像的统计特征的载体图像,将秘密信息嵌入载体图像后,对图像隐写效果进行分析. 经过隐写分析器判别后输出与载体图像相似度极高的载密图像,减少了载体图像的修改痕迹,提高了隐写的隐蔽性,解决了前述问题(4).

2 相关知识

本节主要介绍基于区块链的隐蔽通信和IPFS、基于GAN的隐写术及CP-ABE和环签名的相关知识.

2.1 基于区块链的隐蔽通信和IPFS

区块链是一种链式结构的分布式账本,其中链上的数据是不可被篡改的[18]. 每个节点都不能修改其数据,因为一旦被记录下来,任何块中的数据都不能在没有修改所有后续块的情况下被追溯修改. 节点是基于地址而不是个人身份创建交易. 交易被广播到网络中的每个节点,然后由未花费的交易输出(Unspended Transaction Outputs,UTXO)验证. 一旦这些交易被验证,它们将被打包成块. 当其他节点验证块中包含的所有交易都有效时,该块可以添加到区块链. 最后,所有节点记录交易并达到信息同步状态.

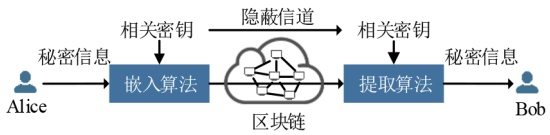


图1 区块链隐蔽通信模型

区块链中的隐蔽通信模型如图1所示. 发送方Alice通过特定的嵌入算法将秘密信息嵌入公共载体中,形成一个包含秘密的载体,该载体将通过隐蔽信道进行传输. 在嵌入秘密信息的过程中,Alice使用密钥K对秘密信息进行加密. 只有Bob可以使用与嵌入过程相同或相关的密钥K提取秘密信息. 在传输过程中,发送方不直接与接收方进行通信,而是随机选择接收地址与区块链网络中的其他普通节点进行通信. 因为交易广播,最终接收方也能收到秘密信息. 这样既不暴露接收方的身份,又保证了通信过程的隐蔽性.

IPFS是一个分布式文件系统,它是基于内容寻址来唯一地标识每个文件. IPFS采用分布式哈希表(Distributed Hash Table,DHT)的索引结构和Merkle有向无环图(Merkle Directed Acyclic Graph,Merkle DAG)的数据结构[19]. 当存储在IPFS对象中的文件超过256 KB时,文件会被分割成几个256 KB的块. 每个块的哈希值作为一个标识符(Content-ID,CID)来识别该块,而且还能用来验证数据是否被篡改. Merkle DAG的根哈希值表示完整的文件. 当发送方将文件上传到IPFS时,IPFS将返回一个用文件内容计算的哈希值. 当接收方希望从IPFS下载文件时,他只需要将文件的哈希值输入到IPFS中,系统就会返回相应的文件. 但是只有在发送方和接收方建立IPFS集群时,接收方才能使用哈希值从IPFS下载文件. IPFS集群分为公有IPFS集群和私有IPFS集群. 公共IPFS集群是一个分布式网络,世界各地的任何IPFS节点都可以参与其中. 私有IPFS集群中的节点只连接到具有共享密钥的其他对等体,并且这些节点不会响应外部访问. 在IPFS网络中,如果一个节点故障,其他节点仍然可以提供所需的文件. 它在很大程度上确保了存储在IPFS上的数据的安全性.

2.2 基于GAN的图像隐写术

GAN是由Goodfellow等人[20]提出的一种生成模型,被广泛地应用于图像的生成. 该模型包括一个生成器(Generator)和一个判别器(Discriminator)[21]. 生成器的任务是从一个随机分布中采样一个噪声,然后输出合成图像. 判别器将一张真实图像或者一张合成图像作为输入,输出判断的结果. 生成器和判别器不断地进行对抗博弈,直到判别器将合成图像判断为真实图像,最终输出以假乱真的生成图像.

基于GAN的图像隐写术借鉴对抗的思想,引入信息隐藏技术. Volkhonskiy等[22]首次将GAN和信息隐写技术结合,在GAN的基础上增加了一个图像隐写术模块和隐写分析模块,如图2所示. 生成器生成符合自然图像的统计特征的合成图像. 判别器判断图像的真假性,若将合成图像判断为真实图像,则将合成图像输入

到图像隐写术模块,用作载体图像. 图像隐写术模块将秘密信息嵌入到载体图像中. 隐写分析模块来区分载体图像和载密图像. 如果无法区分,则将含密图像输出;如果区分出来,则继续训练.

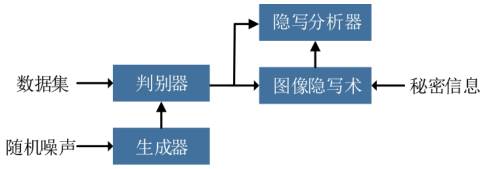


图2　基于GAN的图像隐写术

实际的隐写过程使用传统的隐写术:最低有效位算法(Least Significant Bits,LSB),以保证秘密信息能够提取出. LSB是一种被广泛应用于图像隐写中的信息隐藏算法. 它将每个像素的最低有效位替换为秘密信息. 每个像素由三种原色即红、绿、蓝(RGB)组成,每种颜色占8位. 在嵌入过程中,当要嵌入的秘密信息的位与像素的最低位不同时,将像素的最低位从"1"修改为"0"或从"0"修改为"1". 改变的像素值不影响图像的视觉效果. 该算法不仅易于实现,而且可以隐藏大量的秘密信息.

2.3　CP-ABE和环签名

为了保护敏感文档,需要在对秘密文档进行隐蔽传输之前,对敏感文档进行加密处理,不仅保证了隐蔽性,而且提高了安全性.

Bethencourt等[23]提出了第一个CP-ABE方案,该方案允许数据所有者通过设置访问策略来实现数据的细粒度访问控制. 密文对应于一个访问结构而密钥对应于属性集合,当且仅当属性集合中的属性能够满足此访问结构才能解密[24]. CP-ABE的具体流程如下.

(1) 初始化:输入安全参数,输出公开参数PK和一个主密钥MK.

(2) 加密:输入一个消息m、一个访问结构A、公开参数PK,输出密文E.

(3) 密钥生成:输入一组属性Y、主密钥MK、公开参数PK,输出一个属性Y对应的解密密钥SK.

(4) 解密算法输入:通过传入公开参数PK、密文E和用户解密密钥SK,如果在用户解密密钥SK中包含的属性满足密文E包含的访问结构A时,该算法将密文E解密为明文M.

环签名是由Rivest等人[25]首次提出的一种匿名签名技术,具有无条件匿名性和不可伪造性. 签名者利用自己的私钥和环签名成员中的其他人的公钥进行签名. 即使攻击者在获得环签名成员私钥的情况下,也无法确定签名是环中哪个成员产生的. 本文中,为了隐藏隐蔽通信中发送方身份,发送方在创建区块链交易时采用环签名. 同时为了避免除通信双方外的环签名成员都可以对交易进行验证,本文借鉴环签名的思想,在区块链网络中的发送方Alice创建多个账户作为环签名成员,且只使用其中一个账户创建交易,最后一个环签名成员则是接收方Bob. 如果Bob能对交易验证成功,则表示交易实际上是发给Bob的. 具体的签名过程如下.

(1) 系统参数生成:创建多个账户,并为每个账户生成相应的公钥和私钥.

(2) 签名:在输入消息m和n个环签名成员的公钥$P=\{P_1, P_2, \cdots, P_n\}$以及用于创建交易的账户的私钥$SK$后,对消息$m$产生一个签名$R$,其中$R$中的某个参数根据一定的规则呈环状.

(3) 验证签名:在输入消息m和n个环签名成员的公钥$P=\{P_1, P_2, \cdots, P_n\}$以及签名$R$后,若$R$为$m$的环签名则输出"1",否则输出"0".

3　H-SD&SI框架

在本节中,本文在区块链网络中引入CP-ABE、基于GAN的图像隐写术和环签名,提出了一种可隐藏敏感文档和发送者身份的区块链隐蔽通信模型:H-SD&SI. H-SD&SI的框架如图3所示,它由嵌入过程、传输过程和提取过程三个部分组成.

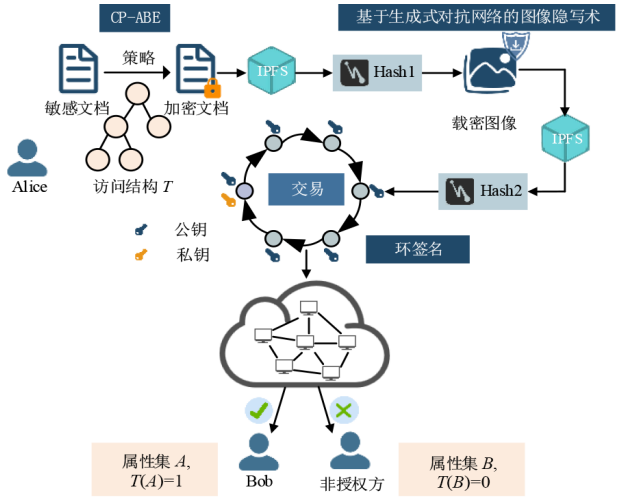


图3　H-SD&SI的框架

3.1　嵌入过程

信息隐藏技术不同于信息加密技术. 信息隐藏技术使未授权方或恶意方不知道秘密信息的存在,而信息加密技术将信息处理成难以理解的数据. 将信息隐藏技术和信息加密技术相结合,不仅可以保证隐蔽性,而且还能提高模型的安全性. 因此,在本文中,敏感文档首先经过信息加密技术处理成加密文档,加密文档再经过信息隐藏技术隐藏在某一载体中,接着进入下一阶段的载体在区块链隐蔽传输过程.

在这一阶段，发送方 Alice 首先需要对敏感文档 secret. pdf 进行 CP-ABE 加密，得到加密文档 secret. pdf. cpabe，接着 Alice 将加密文档上传到至 IPFS. Alice 和接收方 Bob 只有建立 IPFS 集群，Bob 才能根据哈希值从 IPFS 下载文件，因此本文建立私有 IPFS 集群进行存储文件. Alice 创建一个共享密钥 swarm. key，并将其发送给其他节点，包括 Bob. 假设 Alice 和 Bob 事先约定：Bob 接收到 swarm. key 时，表示他知道 Alice 要发送敏感文档. 为了让 Bob 知道何时读取敏感文档，本文引入了计时机制. 在区块链中生成一个块大约需要 10 min，并且每个块包含 2000~3000 个交易，因此本文将时间间隔设置为 10 min. 10 min 之后，Bob 开始遍历新生成的区块.

敏感文档经过 CP-ABE 加密之后得到加密文档，但是加密文档不方便使用信息隐藏技术嵌入某一载体中，本文引入 IPFS 来存储加密文档，仅将 IPFS 返回的加密文档的哈希值嵌入隐写载体中，这样做不仅可以保证隐蔽性和安全性，而且还能使敏感的隐私数据不以明文的形式直接上链.

Alice 将加密文档上传至 IPFS 之后，IPFS 返回加密文档的哈希值. Alice 利用 GAN 生成具有自然图像统计特征的载体图像，将文档的哈希值使用 LSB 算法嵌入载体图像中，得到载密图像. 嵌入过程如图 4 所示，具体的嵌入步骤如下所示.

（1）初始化. Setup(λ)→PK, MSK：该算法将一个安全参数 λ 作为输入，输出一个公钥 PK 和一个主密钥 MSK.

（2）加密. Encrypt(PK, M, P)→C：该加密算法在访问策略 P 下对敏感文档 M 进行加密，将公钥 PK，敏感文档 M 和访问策略 P 作为输入，输出加密文档 C.

（3）上传. Upload(C)→H_1：将加密文档 C 上传至 IPFS 中，返回加密文档 C 的哈希值 H_1.

（4）生成器. Gen(noise)→cover - image：该算法实际上是一个神经网络，称为生成器 Generator，它接收一个随机噪声 noise，尽量生成接近真实的图像，用于后续隐写操作的载体图像 cover - image.

（5）判别器. Dis(real - image, cover - image)→0/1：这一算法实际上也是一种神经网络，被称为判别器 Discriminator. 它的任务是区分真实图像 real - image 和生成的载体图像 cover - image，返回判断结果. 当返回结果为“0”时，代表判别器可以区分出来 real - image 和 cover - image；当返回结果为“1”时，代表判别器无法区分 real - image 和 cover - image，此时的生成图像就可以作为载体图像，供后续隐写操作.

（6）图像隐写. Embed(H_1, cover - image)→stego - image：这一步骤主要使用 LSB 算法将加密文档 C 的哈希值 H_1 嵌入载体图像 cover - image，得到载密图像 stego - image.

（7）隐写分析器. Steganalysis(cover - image, stego - image)→0/1：这一算法的任务是区分生成的载体图像 cover - image 和载密图像 stego - image，返回判断结果. 当返回结果为“0”时，代表判别器可以区分出来 cover - image 和 stego - image；当返回结果为“1”时，代表判别器无法区分 cover - image 和 stego - image.

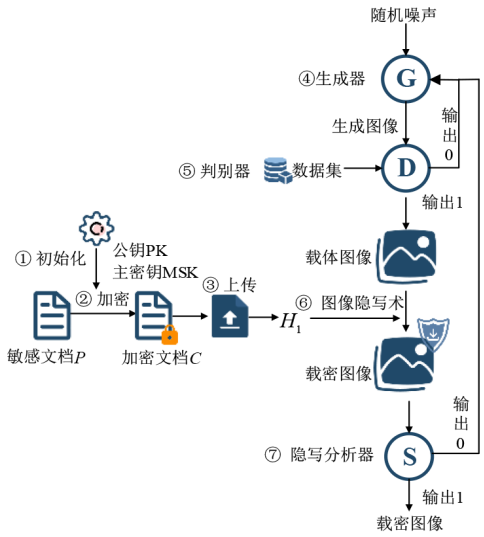


图 4 嵌入过程

3.2 传输过程

如果将载密图像直接存储在区块链上，开销太高；如果将图像压缩存储在区块链上，可能会由于图像失真造成嵌入的秘密信息丢失，因此本文将区块链和 IPFS 结合起来，实现链上和链下的协同存储. IPFS 实现载密图像的链下存储，区块链存储 IPFS 返回的文件的哈希值. 这种协作模式有效地解决了区块链的存储容量问题，而且保证了载密图像的完整性、真实性和安全性.

在这一过程中，Alice 将载密图像上传至 IPFS 中，得到载密图像的哈希值. 接着 Alice 随机选择一个接收地址，而不是直接选择 Bob 的地址，创建一笔交易，将载密图像的哈希值存放到交易的 data 字段. 在对交易环签名之后，将交易广播到区块链网络中，经验证、打包上链，Bob 也能收到交易. 传输过程如图 5 所示，具体的传输步骤如下所示.

（1）上传. Upload(stego - image)→H_2：将载密图像 stego - image 上传至 IPFS 中，返回载密图像 stego - image 的哈希值 H_2.

（2）创建交易. Transaction(H_2)→TX：在该阶段中，Alice 创建一笔交易 TX，交易的 data 字段携带载密

图像 stego - image 的哈希值 H_2.

(3) 环签名. Sign(TX, P_1, P_2, ⋯, P_n)→σ: 该签名算法包括六个步骤. P_1, P_2, ⋯, P_n 分别表示所有环签名成员的公钥,包含 Alice 的公钥 P_s 和 Bob 的公钥 P_b. 在第一步中,使用加密散列函数计算 k=Hash(H),将 k 将用作对称加密密钥. 在第二步中,选择一个随机值 v. 在第三步中,为除了发送方的 n−1 个环签名成员分别选择一个随机值 x_i,并根据 $y_i=g_i(x_i)$ 计算相应的 y_i. 在第四步中,解环方程 $C_{k,v}(y_1, y_2, \cdots, y_n)=v$ 得到 y_s. 在第五步,根据 $x_s=g_s^{-1}(y_s)$ 使用发送方的私钥计算得到 x_s. 在第六步中,环签名 σ 是一个(2n+1)元组 $\{P_1, P_2, \cdots, P_n; v; x_1, x_2, \cdots, x_n\}$.

(4) 提交交易. Submit(TX,σ): Alice 将经过环签名的交易发布到区块链网络,交易在区块链中广播,然后由 UTXO 验证交易是否有效. 当交易被验证有效后,它将被打包到一个块中,通过一个被称为挖矿的过程. 在验证块中包含的所有交易都是有效的之后,区块链网络中的所有节点将更新新生成的块. 最后,接收方还可以接收发送方提交的交易.

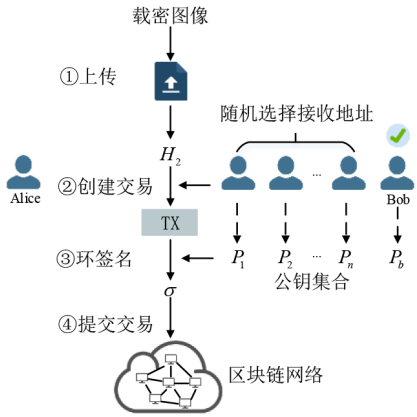


图 5　传输过程

3.3　提取过程

Bob 在接收到 swarm. key 后的 10 min,开始遍历新生成区块中的交易,并尝试验证环签名,如果验证成功,则表示交易实际上是发给 Bob 的. 提取过程如图 6 所示,具体的提取步骤如下所示.

(1) 验证签名. Verify(σ, P_1, P_2, ⋯, P_n)→0/1: 签名验证算法包括三个步骤. 第一步,对于每一个 x_i,计算 $y_i=g_i(x_i)$ 得到相应的 y_i. 第二步,计算对称密钥 k=Hash(H). 第三步,验证环方程 $C_{k,v}(y_1, y_2, \cdots, y_n)=v$ 是否成立. 如果环方程是正确的,则认为签名是正确的,否则认为签名是错误的.

(2) 读取. Read(payload)→H_2: 从交易的 data 字段中读取出载密图像 stego - image 的哈希值 H_2.

(3) 下载. Download(H_2)→stego - image: Bob 输入 H_2 到 IPFS,IPFS 首先通过 H_2 查找和载密图像 stego - image 相关的 DHT 的索引结构,然后通过 DHT 查找保存数据块的节点的位置. 从节点下载载密图像的数据块后,IPFS 将按照 DHT 散列数组的顺序重新组装数据块,并向 Bob 返回完整的载密图像 stego - image.

(4) 提取. Extract(stego - image)→H_1: 从载密图像 stego - image 中提取出加密文档 C 的哈希值 H_1,提取算法是 LSB 嵌入算法的逆过程.

(5) 下载. Download(H_1)→C: Bob 输入 H_1 到 IPFS,IPFS 首先通过 H_1 查找和加密文档 C 相关的 DHT 的索引结构,然后通过 DHT 查找保存数据块的节点的位置. 从节点下载加密文档 C 的数据块后,IPFS 将按照 DHT 散列数组的顺序重新组装数据块,并向 Bob 返回完整的加密文档 C.

(6) 密钥生成. KeyGen(PK, MSK, A)→SK_A: 该算法是密钥生成算法,输入一个公钥 PK,一个主密钥 MSK 和一组请求者的属性集 A,输出与请求者的属性集相关联的解密密钥 SK_A.

(7) 解密. Decrypt(PK, C, SK_A)→M: 该算法是解密算法,传入一个公钥 PK、一个加密文档 C 和解密密钥 SK_A,如果用户的解密密钥 SK_A 中包含的属性满足加密文档 C 包含的访问策略 P 时,则该算法将加密文档解密 C 为明文的敏感文档 M.

图 6　提取过程

4 仿真实验与实验分析

本节介绍了实验过程,并对实验结果进行了分析.本次实验采用 Python 语言在 Ubuntu 16.04 中编写,并使用MNIST数据集和CelebA人脸数据集分别对100个大小不同的敏感文档进行测试.

4.1 仿真实验

在Ubuntu系统中,本实验使用FISCO BCOS模拟区块链,创建20个账户,每个账户的公钥以及地址如表1所示.因篇幅有限不一一列出.

表1 20个账户的公钥和地址

账户	公钥	地址
1	0x07097c450f8ba66fc64436ddc351c696984dc3f80b5e1d4dc567f0a507ef0b3d93d27a94dd4fc5dfb7750b22b6df726eb2f7dba4cc5c693888be6db5d8dd8adb	0xf1420e5F0D8097216615499Fba9BF14F6DB67EA3
2	0x8f7dbda544f48be15695c2fba6ef30f5d6e784199a1a08d1ccdc7bf443d51f77da6974398a6499320d49f26295edfd3a7d2c22e6c5717b49b9b6ce73e4e861f2	0x91CB0D322ba3817CAE7b00f42C004f9C1aFd8bCc
3	0xe23634b6e68b4ad43d8e4c182e68d2092f7225ac6055ec3f0fd5a12f9a9cbe6d1020a95e9640029f6abaf99ff6866b4993f0ce8d3a843d8917ec5dcc734008a6	0xf141187db2EA48d41f222e0D4db3A5bdF567bDb6
4	0x4910ad8dcaeed26969ae6283f5b5fe556430c072a2ae172ad1fc5487d891258110a3825073bc28cd18bb9dd053ff9b34e2e9424179c80e4c1afbb764da10d4be	0xd83932f50C554110D4834f7722625961C752eF4D
5	0x7df08607d62077060779d20acd4ffe4ddc421e85130e97ea6a19dd25a50be7f29e03086db4669a77d247d22983f105b249e446f2723b45216d9bfde65c15d76	0x2dCA0eD57426f36B7251f000Bc6D92D3aA0C3BDd
…	…	…
20	0x0cd5175e55a43ca0b8166dafd1e63facfec46943020c4c059a7ad7897f506667c8a879857b15428a9e9444132c2491aa2b89f24ea10ccb70c76ef761d413718c	0xE925E104fCAe2218fb659A5B97314a1bD2986509

假设账户1是Alice用于创建交易的账户,账户2是Bob的账户,Alice配置本地IPFS节点,并使用JS-IPFS-API调用IPFS服务.Alice生成共享密钥swarm.key,并通过安全通道将swarm.key发送给其他节点,包括Bob.swarm.key的具体内容如下所示.

(1) /key/swarm/psk/1.0.0/

(2) /base16/

(3) 8c45603441c4e23f70714a492f011fa1056e82124f73643 7f28481155ce46ef

通过cpabe-setup命令生成公钥pub_key和主密钥master_key,Alice使用公钥pub_key分别对100个大小不同的敏感文档[secret1.pdf, secret2.pdf, secret3.pdf, …, secret100.pdf]进行加密,如表2所示,得到加密文档[secret1.pdf.cpabe, secret2.pdf.cpabe, secret3.pdf.cpabe, …, secret100.pdf.cpabe],加密文档中暗含了访问控制策略policy.并且利用Bob的属性、公钥pub_key和主密钥master_key,为Bob生成解密密钥bob_priv_key.

区块链网络中包括多个用户(比如User1,User2和User3等),每个用户可以有多个账户地址(比如Address1,Address2和Address3等).另外,区块链网络中可以构建多个私有IPFS集群(比如IPFS1,IPFS2和IPFS3等).因此,本文数据访问控制中属性定义的可选范围如表3所示.

表3 用户属性及属性值的定义

属性	属性值
用户ID	User1,User2,…
账户地址ID	Address1,Address2,…
IPFS集群ID	IPFS1,IPFS2,…

策略是有属性组成的访问结构.本文为了只让授权方Bob解密加密文档,为Bob定制专属的访问策略.策略policy定义为:(用户ID=Bob) and (地址ID=0x91CB0D322ba3817CAE7b00f42C004f9C1aFd8bCc) and (IPFS集群ID=IPFS*),如图7所示.

Alice使用add(·)方法分别将加密文档[secret1.pdf.cpabe, secret2.pdf.cpabe, secret3.pdf.cpab e , …, secret100.pdf.cpabe]上传到IPFS上,IPFS返回它们的哈希

表2 100个大小不同的敏感文档

敏感文档	大小	加密文档	加密文档的哈希值
secret1.pdf	2.03MB	secret1.pdf.cpabe	QmQpvkABZ6hDg5UxcWKNUqS9Nwjoc9YYztLpb62wcsboWY
secret2.pdf	1.14MB	secret2.pdf.cpabe	QmaehxqkiH7Ez2nuXVH8JKqZUCVNsdC4LVmTk3B2GUBqaZ
secret3.pdf	1.68MB	secret3.pdf.cpabe	QmdVy6SBejwp57uiBbrSnbvDapQFsxSqjuUWn3ZYjrRTyU
…	…	…	…
Secret100.pdf	2.06MB	secret100.pdf.cpabe	QmRpXkRacz3NfdwsoWAeDyyLGBQspNHqpsoknGVY4HN2vF

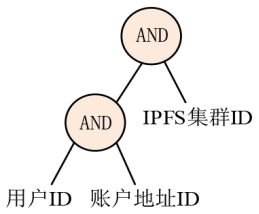


图7　访问控制策略

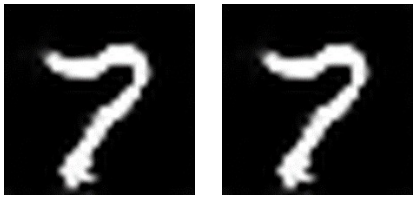
值,如表2的第4列所示. 然后Alice将返回的哈希值转成二进制序列,便于后续嵌入生成的载体图像中. 后续操作以secret1.pdf.cpabe的哈希值H_1为例,将H_1转成二进制序列BS,H_1和BS的具体内容如表3中所示. 为了便于让收方知道嵌入何时结束,双方事先约定在哈希值H_1后面添加一个分隔符d,其具体内容是"/n#",d以及d的二进制序列BS_d如表4中所示.

Alice利用基于GAN的图像隐写术分别训练MNIST数据集和CelebA人脸数据集生成载体图像cover-image 1和cover-image 2,如图8(a)和8(c)所示. 接着,Alice将BS和BS_d嵌入生成的载体图片cover-image 1和cover-image 2中,得到载密图像stego-image 1和stego-image 2,如图8(b)和8(d)所示,嵌入前后对比如图8所示. 然后Alice将载密图像stego-image 1和stego-image 2上传到IPFS上,IPFS返回载密图像stego-image 1的哈希值H_2^1和载密图像stego-image 2的哈希值H_2^2,H_2^1和H_2^2的具体内容如表3中所示.

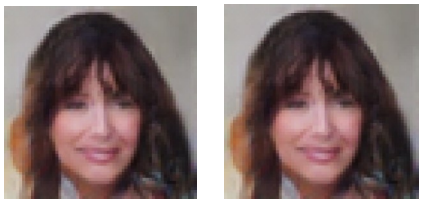
Alice没有直接选择Bob的帐户,而是随机选择一个接收地址创建交易,交易中的data字段携带载密图像stego-image的哈希值H_2. Alice对交易进行环签名,环签名结果写入交易的extraData字段,并将交易发布到区块链网络. 交易被验证之后,被打包成块. 区块链网络中的所有节点更新新生成的块. 最后,Bob也可以接收到Alice提交的交易. 交易结构如下所示.

① signedTransaction ={

② nonce=1,



(a) cover-image 1　　(b) stego-image 1



(c) cover-image 2　　(d) stego-image 2

图8　嵌入前后对比

③ gasPrice=300000000,

④ gas=300000000,

⑤ blockLimit=502,

⑥receiveAddress=accounts[random.randint(1,20)].address,

⑦ value=0,

⑧data='QmVUPp1SWGA9nsBwvjdrb6oFNyhe28 huhpw4W4B9CHUAJQ',

⑨ extraData=' {"message": "QmVUPp1SWGA9nsBwvjdrb6oFNyhe28huhpw4W4B9CHUAJQ"\, "param_info": " {\"g\": \"2. \"\, \"p\": \"116629146130897……085687.\"\, \"q\":\"583145730654485178 76……542843.\"} "\, "ret_code": 0\, "sig": " {\"C\": \"596934492704……849502.\"\, \"Y\": \"631573589796……098535.\"\, \"num\":\"3\"\, \"pk0\":\"114228877694……654739.\"\, \"pk1\":\"4751250745535584……301670. \"\, \"pk2\":\"7401228587……502970. \"\, \"s0\": \"53226645683501……384828.\"\, \"s1\":\"2403484418121……539097.\"\, \"s2\":\"1610471047……137130.\"}"}'}

表4　相关的符号及其内容

符号	内容
H_1	QmQpvkABZ6hDg5UxcWKNUqS9Nwjoc9YYztLpb62wcsboWY
BS	0101000101101101010100010111000001110110011010110100000101000010010110100011011001101000010001000110011100110101010101010111100001100011010101110100101101001110010101010111000101010011001110010100111001110111010101001101111011000110011100101011001010110010111101001110100010011000111000001100010001101100011001001110111011000110111001101100010011011110101011011101011001
d	/n#
BS_d	00101111011011100010001 1
H_2^1	QmVUPp1SWGA9nsBwvjdrb6oFNyhe28huhpw4W4B9CHUAJQ
H_2^2	QmX8oKoh78C4Y1GrVFqdG6hqkrzQkWZtF1hSNdvMaL8gHD

为了让Bob能查到Alice提交的交易，双方事先约定data字段中有“Qm”开头的交易即为Alice提交的交易. Bob在收到共享密钥swarm. key的10 min后，开始遍历新生成的块，查找data字段中有“Qm”开头的交易. 找到交易后，Bob先验证环签名，验证通过后，读取交易的data字段，将data字段的内容输入IPFS，获取完整的载密图像. 根据LSB算法的提取算法从载密图像中提取出加密文档的哈希值，再将加密文档的哈希值输入IPFS，IPFS返回完整的加密文档. 最后Bob根据自己的属性集(Bob, 0x91CB0D322ba3817CAE7b00f42C004f9C1aFd8bCc, IPFS*)获得解密密钥，解密加密文档得到敏感文档.

4.2 实验分析

本小节主要从隐藏容量、隐蔽性和安全性这三个方面对实验结果进行分析.

(1)传输秘密信息容量

本文对100个不同大小的敏感文档分别进行仿真实验操作，将这些敏感文档进行加密后上传至IPFS，并成功地将IPFS返回的哈希值嵌入载体图像中进行隐蔽传输. 相比于以往只能传递一条消息的研究，文本提出的方法在传输数量级上有很大的提高，传输的秘密信息量可达到MB. 区块链隐蔽通信模型中各方法的传输秘密信息量对比如表5所示.

表5 传输秘密信息量对比

方法	容量
文献[6]	bit
文献[7]	KB
文献[8]	bit
文献[9]	bit
本文	MB

(2)隐蔽性

隐蔽性主要是指载体图像和载密图像的统计特征的相似性，主要使用均方误差(Mean-Square Error, MSE)、峰值信噪比(Peak Signal to Noise Ratio, PSNR)和结构相似性(Structural Similarity Index, SSIM)来进行评估.

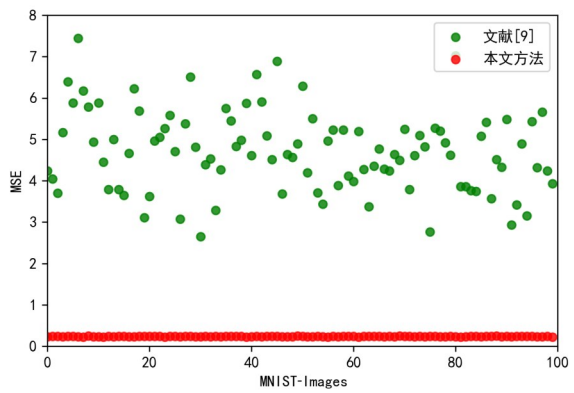
均方误差(MSE)主要是反映载体图像与载密图像之间的差异程度，使用这个指标来衡量嵌入秘密信息之后得到的载密图像的质量. 通过将载体图像和载密图像的所有像素值差的平方和除以像素的总数来计算均方误差. MSE值越小，隐写方法越好. MSE的公式表示如下：

$$\mathrm{MSE}=\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{(I(i,j)-I'(i,j))^2}{M*N} \tag{1}$$

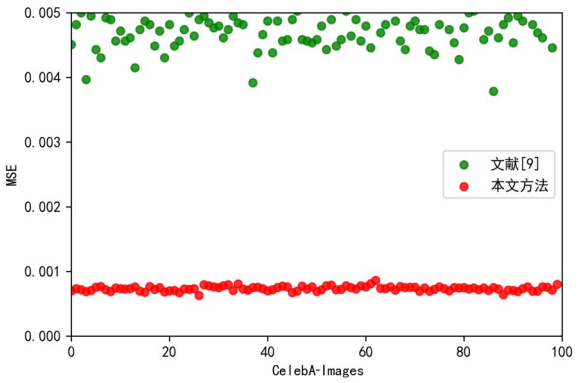
其中，i和j分别表示图像的行和列；$I(i,j)$表示载体图像中第i行、第j列的像素；$I'(i,j)$表示载密图像中第i行、第j列的像素.

文献[9]使用的是传统的图像隐写术LSB，本文使用的是基于GAN的图像隐写术. 本文将文献[9]中的隐写方法和本文方法作对比，分别将秘密信息嵌入普通载体和由MNIST数据集生成的100张载体图像中，并计算载体图像和载密图像之间的MSE，如图9(a)所示. 本文方法的MSE在0.2左右，远低于传统隐写方法的MSE. 同样地，分别将秘密信息嵌入普通载体和由CelebA人脸数据集生成的100张载体图像中，并计算载体图像和载密图像之间的MSE，如图9(b)所示. 本文方法的MSE远低于文献[9]的MSE，即本文隐写方法的隐蔽性要好于文献[9]的隐写方法.

峰值信噪比(PSNR)这个指标来衡量秘密信息嵌入图像之后得到的载密图像的质量. 与MSE相反，PSNR值越大，图像的质量越好. 它的单位是dB，当PSNR的值高于40 dB时，说明图像质量极好，非常接近原始图像；当PSNR的值介于30 dB和40 dB之间时，说明图像质量较好，可以察觉到图像失真但可以接收；当PSNR的值介于20 dB和30 dB之间时，说明图像质量



(a) MNIST数据集



(b) CelebA人脸数据集

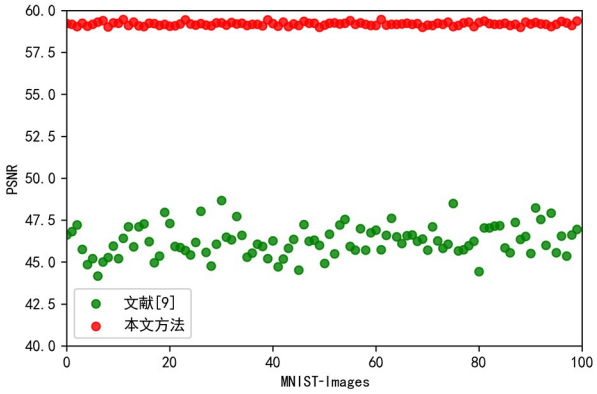
图9 均方误差的对比

差;当PSNR的值低于20 dB,说明图像不可接收.

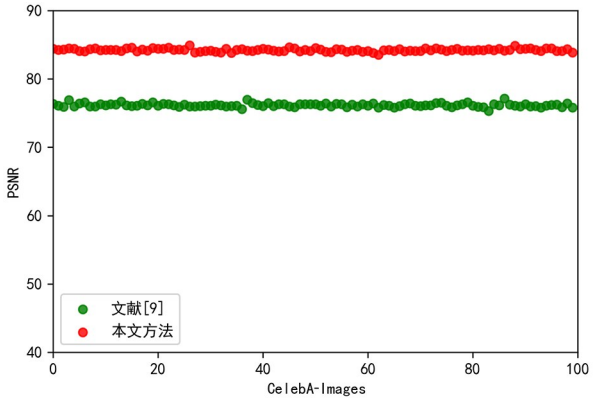
PSNR的公式表达如下:

$$\mathrm{PSNR}=10\lg\frac{255^2}{\mathrm{MSE}} \tag{2}$$

本文将文献[9]中的隐写方法和本文方法作对比,分别将秘密信息嵌入普通载体和由MNIST数据集生成的100张载体图像中,并计算载体图像和载密图像之间的PSNR,如图10(*a*)所示. 同样地,分别将秘密信息嵌入普通载体和由CelebA人脸数据集生成的100张载体图像中,并计算载体图像和载密图像之间的MSE,如图10(*b*)所示. 本文方法的PSNR远高于文献[9]所用的隐写方法的PSNR,即本文隐写方法的隐蔽性要好于文献[9]的隐写方法.



(*a*)　MNIST数据集



(*b*)　CelebA人脸数据集

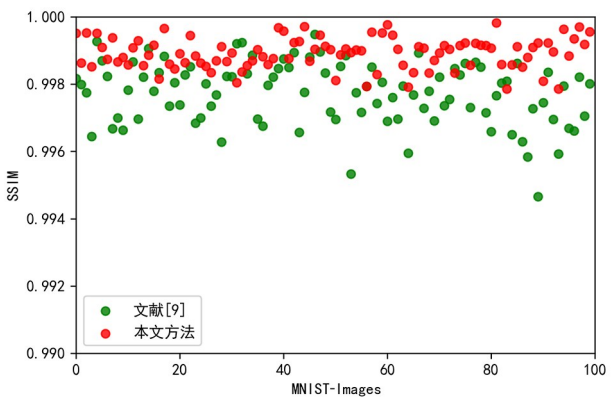
图10　峰值信噪比的对比

结构相似性(SSIM)是一种衡量两幅图像相似度的指标[26]. SSIM的最大值为1. SSIM值越大,载体图像和载密图像相似性越高. SSIM的公式表达如下:

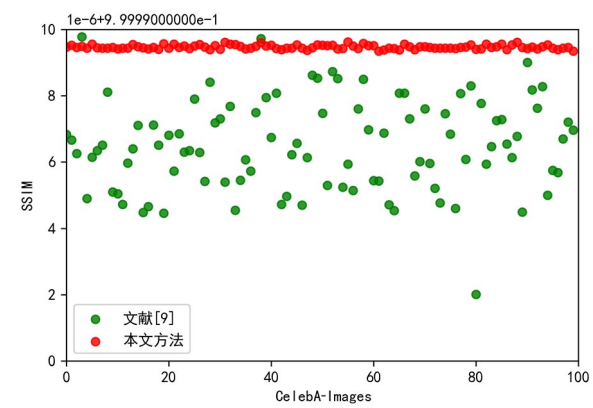
$$\mathrm{SSIM}(x,y)=\frac{(2\mu_x\mu_y+C_1)(\sigma_{xy}+C_2)}{(\mu_x{}^2.\mu_y{}^2+C_1)(\sigma_x{}^2+\sigma_y{}^2+C_2)} \tag{3}$$

其中,μ_x代表x的平均值;μ_y代表y的平均值;$\sigma_x{}^2$代表x的方差;$\sigma_y{}^2$代表y的方差;σ_{xy}代表x和y的协方差;$C_1=(k_1L)^2$和$C_2=(k_2L)^2$是用来维持稳定的常数,L是像素值得动态范围,$k_1=0.01$,$k_1=0.03$.

本文将文献[9]中的隐写方法和本文方法作对比,分别将秘密信息嵌入普通载体和由MNIST数据集生成的100张载体图像中,并计算载体图像和载密图像之间的SSIM,如图11(*a*)所示. 本文方法的SSIM接近于1,而且高于文献[9]所用的隐写方法的SSIM,即使用本文方法得到的载密图像与载体图像相似性极高,隐蔽性要好于文献[9]的隐写方法. 同样地,分别将秘密信息嵌入普通载体和由CelebA人脸数据集生成的100张载体图像中,并计算载体图像和载密图像之间的SSIM,如图11(*b*)所示. 本文方法的SSIM高于文献[9]所用的隐写方法的SSIM,同样可以得出本文方法的隐蔽性要好于文献[9]中的隐写方法这一结论.



(*a*)　MNIST数据集



(*b*)　CelebA人脸数据集

图11　结构相似性的对比

(3)安全性

定义1:　(S1安全性)是指攻击者没有足够的信息证明经过传输信道的载体信息中隐藏有秘密信息.

该类安全性要求隐蔽通信满足不可区分性. 本文用于隐写术的载体图像是由基于GAN的图像隐写术生

成的,载体图像和载密图像的统计特征极为相似,在秘密信息的隐蔽传输过程中,不易让攻击者发现含有秘密信息的载体,保证了安全性.

定义2: (S2安全性)是指通信信息受到主动攻击的情况下仍然能够正确接收到秘密信息.

该类安全性是指攻击者无法损坏经过传输信道的通信信息中所隐藏的秘密信息,即受到攻击者攻击的情况下仍然能够从通信信息中恢复秘密信息. 首先,区块链的不可篡改性使得隐蔽通信的攻击者对秘密信息的删除和篡改都是无效的. 其次,本文在隐写之前使用CP-ABE对敏感文档进行加密,只有当用户的属性通过了访问控制策略的验证时,用户才能对加密文档进行解密,抵御了用户合谋攻击. 而且模型的安全性在一定程度上取决于使用的密钥的机密性,CP-ABE根据用户属性生成解密密钥,避免了私钥泄露. 最后,在本文的区块链隐蔽通信中,发送方和接收方身份都被隐藏,攻击者很难发现含有秘密信息的交易. 攻击者即使怀疑图像中秘密信息,在不知道提取算法的情况下也很难提取出秘密信息,而且在不知道解密密钥的前提下,也无法获取到敏感文档. 由此,保证了隐蔽通信的安全性.

5 总结

本文提出了一种可隐藏敏感文档和发送者身份的区块链隐蔽通信模型H-SD&SI,以实现敏感文档在区块链中的隐蔽传输. 该模型采用CP-ABE技术来提高敏感文档的安全性,并使用环签名技术对交易进行签名来隐藏发送方身份,以提高传输的隐蔽性. 此外,在具体的嵌入过程中,该模型使用基于GAN的图像隐写术将加密文档的哈希值嵌入生成的载体图像中,进一步提高隐蔽性. 本文通过对比载体图像和载密图像的MSE,PSNR和SSIM来评估模型的性能. 实验结果表明,该模型在传输秘密信息量上有很大提升,而且具有较高的隐蔽性和安全性. 然而该模型也存在一定的局限性,即在保证隐蔽性和安全性的情况下,传输敏感文档的实时性相对较差. 在今后的工作中,将考虑对模型进行改进以突破这一局限.

参考文献

[1] SUBHEDAR M S, MANKAR V H. Current status and key issues in image steganography: A survey[J]. Computer Science Review, 2014, 13-14: 95-113.

[2] HUSSAIN M, WAHAB A W A, IDRIS Y I B, et al. Image steganography in spatial domain: A survey[J]. Signal Processing: Image Communication, 2018, 65: 46-66.

[3] DAI H N, ZHENG Z B, ZHANG Y. Blockchain for internet of things: A survey[J]. IEEE Internet of Things Journal, 2019, 6(5): 8076-8094.

[4] FENG Q, HE D B, Zeadally S, et al. A survey on privacy protection in blockchain system[J]. Journal of Network and Computer Applications, 2019, 126: 45-58.

[5] MONRAT A A, SCHELÉN O, ANDERSSON K. A survey of blockchain from the perspectives of applications, challenges, and opportunities[J]. IEEE Access, 2019, 7: 117134-117151.

[6] PARTALA J. Provably secure covert communication on blockchain[J]. Cryptography, 2018, 2(3): 18.

[7] BASUKI A I, ROSIYADI D. Joint transaction-Image steganography for high capacity covert communication[C]// 2019 International Conference on Computer, Control, Informatics and its Applications(IC3INA). Tangerang: IEEE, 2019: 41-46.

[8] LIU S, LIU Y X, FENG C, et al. Blockchain privacy data protection method based on HEVC video steganography [C]//2020 3rd International Conference on Smart BlockChain(SmartBlock). Zhengzhou: IEEE, 2020: 1-6.

[9] SHE W , HUO L J, TIAN Z, et al. A double steganography model combining blockchain and interplanetary file system [J]. Peer-to-Peer Networking and Applications, 2021, 14 (5): 3029-3042.

[10] YUAN C , XU M X, SI X M, et al. Blockchain with accountable CP-ABE: How to effectively protect the electronic documents[C]//2017 IEEE 23rd International Conference on Parallel and Distributed Systems(ICPADS). Shenzhen: IEEE, 2017: 800-803.

[11] HU D H, WANG L, JIANG W J, et al. A novel image steganography method via deep convolutional generative adversarial networks[J]. IEEE Access, 2018, 6: 38303-38314.

[12] HAYES J, DANEZIS G. Generating steganographic images via adversarial training[EB/OL]. (2017-05-01) [2021-08-01]. https://arxiv.org/abs/1703.00371.

[13] YANG J H, LIU K, KANG X G, et al. Spatial image steganography based on generative adversarial network [EB/OL]. (2018-04-21)[2021-08-01]. https://arxiv.org/abs/1804.07939.

[14] LIU J, KE Y, ZHANG Z, et al. Recent advances of image steganography with generative adversarial networks[J]. IEEE Access, 2020, 8: 60575-60597.

[15] SHI H C, DONG J, WANG W, et al. SSGAN: Secure

steganography based on generative adversarial networks [C]//Advances in Multimedia Information Processing - PCM 2017. Harbin: Springer, 2018: 534-544.

[16] LI X F, MEI Y R, GONG J, et al. A blockchain privacy protection scheme based on ring signature[J]. IEEE Access, 2020, 8: 76765-76772.

[17] LI X Q, JIANG P, CHEN T, et al. A survey on the security of blockchain systems[J]. Future Generation Computer Systems, 2020, 107: 841-853.

[18] GAO W C, HATCHER W G, YU W. A survey of blockchain: Techniques, applications, and challenges[C]//2018 27th International Conference on Computer Communication and Networks(ICCCN). Hangzhou: IEEE, 2018: 1-11.

[19] CHEN Y L, LI H, LI K J, et al. An improved P2P file system scheme based on IPFS and Blockchain[C]//2017 IEEE International Conference on Big Data(Big Data). Boston: IEEE, 2017: 2652-2657.

[20] GOODFELLOW I J, POUGET-ABADIE J, MIRZA M, et al. Generative adversarial networks[EB/OL]. (2018-04-21) [2014-06-10]. https://arxiv.org/abs/1406.2661.

[21] WANG K F, GOU C, DUAN Y J, et al. Generative adversarial networks: Introduction and outlook[J]. IEEE/CAA Journal of Automatica Sinica, 2017, 4(4): 588-598.

[22] DENIS V, IVAN N, EVGENY B. Steganographic generative adversarial networks[C]//Twelfth International Conference on Machine Vision(ICMV 2019). Amsterdam: SPIE, 2020: 1-15.

[23] BETHENCOURT J, SAHAI A, WATERS B. Ciphertext-policy attribute-based encryption[C]//2007 IEEE Symposium on Security and Privacy(SP'07). Berkeley: IEEE, 2007: 321-334.

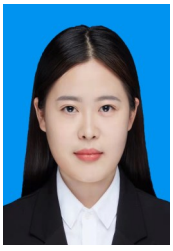
[24] 陈露, 相峰, 孙知信. 基于属性密码体制的区块链安全技术研究进展[J]. 电子学报,2021, 49(1): 192-200.
CHEN L, XIANG F, SUN Z X. A survey of blockchain security technologies based on attribute-based cryptography[J]. Acta Electronica Sinica, 2021, 49(1): 192-200. (in Chineses)

[25] RIVEST R L, SHAMIR A, TAUMAN Y. How to leak a secret[C]//Advances in Cryptology-ASIACRYPT 2001. Gold Coast: Springer, 2001: 552-565.

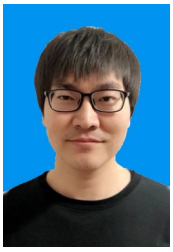
[26] KARAKUS S, AVCI E. A new image steganography method with optimum pixel similarity for data hiding in medical images[J]. Medical Hypotheses, 2020, 139: 109691.

作者简介

佘　维　男,1977年12月生,湖南常德人. 博士,教授,博士生导师,CCF会员. 主要研究方向为区块链技术、信息安全和可信分布式系统.
E-mail: wshe@zzu.edu.cn



霍丽娟　女,1997年6月生,河南开封人. 硕士研究生,CCF会员. 主要研究方向为区块链技术和网络空间安全.
E-mail: lijuan.huo.zzu@outlook.com



田　钊(通讯作者)　男,1985年9月生,河南荥阳人. 博士,讲师. 主要研究方向为区块链技术.
E-mail: tianzhao@zzu.edu.cn