

基于计算机视觉的跨网传输技术

彭 晨¹ 张 磊² 陶 涛¹ 王 婷¹ 闫鑫飞^{2*}

1. 中国电子口岸数据中心南京分中心 南京江苏 210000

2. 南京轩宁信息技术有限公司 南京江苏 210000

摘 要: 随着计算机技术的飞速发展, 信息网络已经成为社会发展的重要保证。为了避免信息泄露, 在一些包含敏感信息尤其是国家机密的场景中, 很多重要部门均采用物理隔离来确保数据安全。随着信息化建设的稳步推进, 跨网数据传输的需求日益显著。因此, 如何有效、快速地在没有物理连接的内网与内网、内网和外网之间传输信息是目前亟需解决的问题。本文基于计算机视觉技术提出了一种将数据编码为图像及从图像中解码数据的方法, 并在此基础上设计出一种使用显示屏和摄像头在两网络之间传输数据的方案, 以在物理隔离的网络之间实现数据的近实时传输。

关键词: 跨网传输; 物理隔离; 图像编码; 信息安全

Cross-network transmission technology based on computer vision

Chen Peng¹, Lei Zhang², Tao Tao¹, Ting Wang¹, Xinfei Yan^{2*}

1. Nanjing branch of china electronic port data center, Nanjing, Jiangsu, 210000

2. Nanjing XuanNing Information Technology Co., LTD, Nanjing, Jiangsu, 210000

Abstract: With the rapid advancement of computer technology, information networks have become a vital assurance for societal development. To prevent information leakage, many crucial sectors, especially those involving sensitive information or national secrets, employ physical isolation to ensure data security. As the drive toward informatization steadily progresses, the demand for cross-network data transmission has grown significantly. Consequently, an urgent challenge is how to efficiently and swiftly transmit information between isolated intranets, intranets, and the internet, without the presence of physical connections. This paper proposes a method based on computer vision technology to encode data into images and decode data from images. Building upon this foundation, a solution is devised that employs displays and cameras to facilitate data transmission between two networks. This approach enables near-real-time data transmission between physically isolated networks.

Keywords: Cross-network transmission; Physical isolation; Image coding; Information security

随着计算机技术的飞速发展, 信息网络已经成为社会发展的重要保证。Internet是一个开放的、无控制机构的网络, 黑客经常会侵入网络中的计算机系统, 窃取或破坏重要数据。为了避免信息泄露, 很多重要部门会有自己的防火墙和安全防护, 但是面对一些顶级的黑客, 这些防护措施并不能保证信息的绝对安全。因此在一些包含敏感信息尤其是国家机密的场景中, 均采用将不同网络进行隔离的方式来确保数据安全。^[1]

目前对网络进行隔离的概念主要包括: 协议隔离、

网络隔离和物理隔离。协议隔离是指任何应用协议均无法在两个网络之间流通, 跨网的数据交换以文件形式进行。网络隔离是指两个网络之间不存在可通的网络连接, 任何应用协议经内部协议封装后实现数据交换。物理隔离是指两个网络之间不存在物理连接, 相应地也不存在任何网络连接。^[2]

网络隔离和协议隔离是物理隔离的弱化概念, 在信息安全场景中物理隔离是目前最常用的手段。随着信息化建设的推进和业务需求的发展, 各党政军机关为提升工作效率, 基于跨部门跨网络的数据开展相应工作已成为不可逆转的趋势, 跨网数据交换也逐步呈现出频次高、

课题资助: 南京海关科研项目 (2023KJ42)

时效性要求强、数据类型多等特点。为保障网络安全,如何在没有物理连接的网络之间快速有效地传输数据,已成为各单位信息化建设中亟需解决的问题。

一、主流跨网数据传输方案

目前跨网数据传输的实现手段主要分为三大类:人工跨网数据传输、半自动跨网数据传输和全自动跨网数据传输。人工跨网数据传输以光盘和专用U盘为代表,半自动跨网数据传输以光盘摆渡机为代表,全自动跨网网数据传输主要包含网闸、单向光闸、码图类摆渡系统等。

1. 人工跨网数据传输

人工跨网数据传输是目前跨网数据交换场景中最常见的手段,其安全性依赖于附加的管理和审核机制。人工跨网数据传输一般由数据接收者或数据提供者发起申请,经业务部门和安全主管部门审批通过后使用专用U盘或光盘装载数据,再安排专人进行数据交接。

人工跨网数据传输以人为责任主体,由专人负责内容审查、递送及数据的安全性,其前提是充分信息经办人,仅适用于数据时效性要求不高的场景。处于介质内的数据无法防止内容复制,数据递送过程中难以控制数据的流向且无法审计,介质存在丢失的风险,这将为数据安全带来隐患。

2. 半自动跨网数据传输

基于光盘摆渡机的跨网数据传输方案一般包含源数据导出服务器、光盘摆渡机和目标数据导入服务器等三个部分。其实现原理是,将光盘接入源数据导出服务器中刻录需要传输的数据,再利用机械臂将光盘切换到目标数据导入服务器中并读取光盘中的存储信息。^[3]

光盘摆渡机适用于网络接口距离较近的两网络之间的数据跨网传输,省去了人工递送过程。光盘摆渡机的安全仍是依赖于人员管理和内容审查,数据刻录过程是由人工完成的,需要对其所刻录的数据进行审查,否则难以保证数据的合规性,也无法保证数据是否被篡改。光盘摆渡机对数据的传输及使用流程无法追溯,且需要大量消耗光盘类耗材。

3. 全自动跨网数据传输

(1) 网闸

对数据传输时效性要求高的在线跨网业务系统需要使用全自动跨网数据传输方案,目前最常用的方案是网闸。网闸一般由内网处理单元、外网处理单元和隔离交换控制单元三部分构成,隔离交换控制单元处于内、外网处理单元之间,并与内、外网处理单元保持物理连接,如图1所示。网闸的工作原理是隔离交换控制单元分时与内、外网单元建立连接,使得同一时刻只与一个网络连接,从数据源网络中获取数据后暂存在中间数据交换区,再将数据推送到目标网络中。^[4]

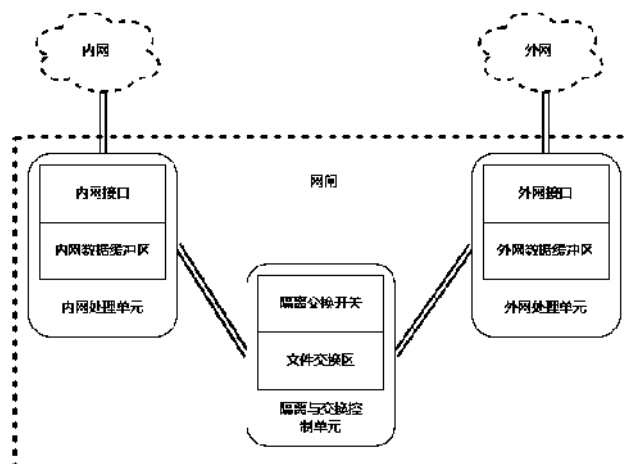


图1 网闸技术原理图

目前网闸多提供服务代理功能,各种应用协议可以直达网闸接口,网闸的内外接口可解析各种应用协议,从中剥离数据或重新封装后转发到另一网络,从应用层面来说,相当于在内外网之间建立了逻辑连接。具有协议代理功能的网闸类似于逻辑上的安全网关,可满足数据交换的需求,但却改变了网络隔离的状态,其安全性依赖于配套的信息安全防护系统。

小部分狭义网闸不提供任何协议代理服务,仅以文件形式进行数据交换,实现了协议隔离。网闸使用逻辑开关来实现两网络之间的网络隔离,在其工作过程中两网络之间一直存在物理连接。另外,网闸是数据双向传输的技术方案,对于要求数据单向传输的场景也依赖于软件层面通过逻辑来实现。因此,网闸的安全性严重依赖于配套的网络安全防护体系。

(2) 单向光闸

单向光闸一般由内网处理单元、外网处理单元和单根光纤组成,通过单根光纤连接数据发送方的发光器和数据接收端的收光器,从而物理上实现数据单向跨网传输,如图2所示。同传统的网闸相比,单向光闸的安全性更高,但不足的是,单向光闸并不能实现两网络之间的物理隔离。^[5]

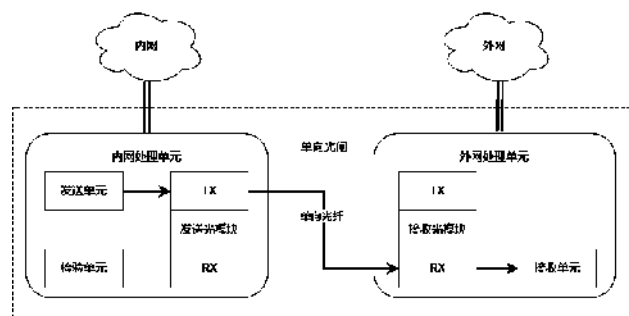


图2 单向光闸技术原理图

(3) 码图类摆渡系统

码图类摆渡系统一般由发送端处理单元和显示屏、接收端处理单元和摄像头构成,其工作原理为:发送端

获取需要跨网传输的数据后编码为图像，并在显示屏上展示编码图像；接收端使用摄像头采集图像并从拍摄图像中解码原始数据，如图3所示。这类系统在整个工作过程中不改变两网络物理隔离的状态，且可在物理层面实现数据单向传输。^[6]

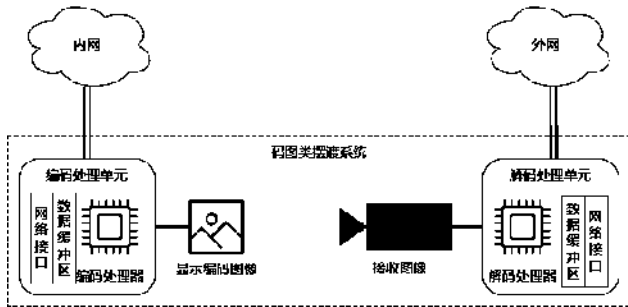


图3 码图类摆渡系统技术原理图

目前，几乎所有码图类摆渡系统均使用二维码作为数据编码图像。二维码是标准的数据图像编解码方案，现有QR码总共有40种规格，最小的是21*21，最大的是177*177；最大的QR码在最低纠错等级时最多只能表示7089个纯数字，或者4276个字母，或者2953个字节（相当于2.9kb）；故当二维码传输大量信息时，由于一张二维码能够存储的信息有限，导致信息传输速度比较慢，不能满足实时性的要求。这类系统提升传输速度的方案只有一种，即多通道并发传输，这也导致了高昂的硬件成本。目前码图类摆渡系统的传输速度基本不超过1Mbps，多数情况下速度更低。^[7-10]

二、基于计算机视觉的跨网传输技术

1. 图像编解码

为了提高单幅图像的数据容量，本文提出了一种新的数据图像编码方式，预设编码图像尺寸为a*b，以白色为背景区，黑色为前景区；预定义 2^n 种图案作为码元，

每个图案用 $m*m$ 的像素块来显示，对应n个比特位的取值，m为不小于n+2的整数。

综合考虑数据的传输量和传输速率，以预设图像尺寸1280*800为例，预定义 $2^7=128$ 种图案，每个图案用9*9的像素块来显示，对应7个比特位的取值，则单幅编码图像中每行可容纳预定图案数为1280/9=142个，每列可容纳预定图案数为800/9=88个，则全图可容纳预定图案数为142*88=12496个，对应数据量为12496*7/8=10934个字节。

图像解码时，将二值化后的图像按顺序分割成9*9的像素块，利用SVM识别每个方块对应的图案，并根据预定义的对对应关系，将每个图像以7个比特位代替，得到接收数据字节流。

2. 数据编码方式

每个编码图像类似于网络中的单个报文，其中包含报文头、数据头和待传输数据。报文头包含报文类型、本端时序号、对端时序号、数据头长度、数据区CRC、数据头CRC和报文头CRC信息；数据区CRC、数据头CRC和报文头CRC用于判定每部分的解码是否正确，保障数据的准确性。数据头包含文件总分片数、分片ID、文件长度、数据区长度、已发送字节数和文件名信息，用于确定待传输数据的拆分情况及传输进度。如表1所示。

3. 跨网传输流程

本技术采用自主研发的、安全可靠的数据编码技术，利用显示屏和摄像头进行内外数据的自动迁移。数据流出方将数据编码为图像后展示在显示屏上，数据流入方使用摄像头获取图像后解码成原始数据。

本技术由发送端和接收端组成，每端均包含处理器、副显示屏和摄像头。发送端副显示屏用以展示数据，接收端副显示屏用以展示校验信息。两端摄像头分别采集

表1 单幅图像中的数据格式

区域	字段号	字段名	字节数	说明
报文头 (字节数: 23, 占用编码图像中第1行)	1	报文类型	1	1: 数据报; 2: 等待传输报
	2	本端时序号	4	本端发送本报文时的时序, 毫秒级
	3	对端时序号	4	本端收到对端上次报文的时序, 毫秒级
	4	数据头长度	2	数据头部分的长度
	5	数据区CRC	4	数据区的CRC校验值
	6	数据头CRC	4	数据头的CRC校验值
	7	报文头CRC	4	报文头的CRC校验值, 不含本字段
数据头 (字节数: 20~248, 占用编码图像中第2和3行)	8	文件总分片数	4	大文件被拆分成多个分片发送。当前文件的总分片数
	9	分片ID	4	当前分片的ID
	10	文件长度	4	当前文件中包含的字节数
	11	数据区长度	4	当前分片中发送文件数据的字节数
	12	已发送字节数	4	在当前分片之前, 当前文件已发送的字节数, 不含当前分片中文件数据
	13	文件名	变长	当前文件名, 变长
数据区	14	文件数据	变长	最大10561个字节, 占用编码图像中第4~88行

对端副显示屏展示的图像。系统架构如图4所示。

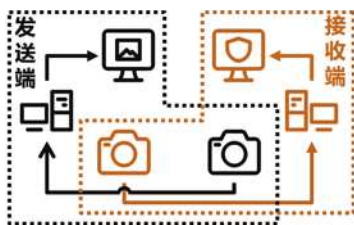


图4 基于计算机视觉的跨网传输技术方案架构图

本技术方案的工作流程为：

- 1) 发送端处理器实时获取待发送的数据并生成校验信息，将数据和校验信息编码为图像并展示在副显示屏；
- 2) 接收端摄像头实时拍摄数据图像；
- 3) 接收端处理器从图像中解码数据并校验，将校验结果编码为图像展示在副显示屏；
- 4) 发送端摄像头实时拍摄校验结果图像；
- 5) 发送端处理器从图像中解码校验结果，据此重发错误数据，或发送后续数据。

根据传输数据的大小不同，按预设的编码方式可能形成多个图像码，每个图像码中都包含一部分需要传输的数据以及该部分数据的序号、名称、总数、字节数、校验码等信息。

(1) 发送端将数据编码为图像的处理流程

1) 读取需要传输数据，根据需要传输数据大小和单幅图像最大编码数据量（指编码图像中数据区可存放的数据量）将需要传输数据拆分为多个分片。

2) 依次按序编码每个分片，即将每一个分片中需要传输的数据写入字节流，依次取7个比特根据其取值按预定义的对对应关系生成一个9*9编码图案，并将所有编码图案按照由左至右，由上至下的顺序存入编码图像第4-88行的数据区；然后在此编码图像的第1行添加与分片相对应的报文头对应的编码图案，在第2-3行添加与分片相对应的数据头对应的编码图案；最终形成与分片数量相同的图像码。

3) 在数据屏幕上显示图像码，并等待接收端的确认信息。

(2) 接收端从图像解码数据的处理流程

1) 接收端通过摄像头拍摄发送端副屏幕上显示的图像码。

2) 接收端对所述图像码图像进行灰度化，并根据编码图像到摄像机图像的变换关系生成待解码图像。编码图像到摄像机图像的变换关系可在前期进行确定，可根据张氏标定法，利用棋盘格图像对摄像头进行相机标定，从而计算出编码图像坐标系中各像素点到摄像头成像坐标系中对应位置的变换关系。^[1]

3) 将待解码图像（即灰度编码图像）二值化，根据编码图像格式逐步解码报文头、数据头和数据区，每解

码一部分则检验CRC，若CRC错误则解码失败，重新将待解码图像二值化或返回步骤1）重新拍摄图像码；若连续多次解码错误，则判定需要重新校准；若重新校准后仍解码错误，则判定当前数据无法接收；若解码成功，生成原始数据。

4) 根据解码情况生成以二维码格式编码的确认信息，形成二维码，并在接收端的副屏幕上显示二维码，若解码成功，则接收所述图像码携带的数据。

由于设计时对报文头、数据头和数据区三个部分都增加了CRC校验码（循环校验码），每解码一部分则检查CRC是否一致，若发生错误则停止解码。即解码时，可分块对待解码图像进行转换和二值化，由于第一部分（即报文头）的内容较少，转换和二值化的速度很快，如果是重复图片或者解析错误，就无须执行第二部分（即数据头）和第三部分（即数据区）的图像，避免冗余的转换和二值化，进一步提升传输效率。

(3) 接收端校验数据的处理流程

接收端解码成功后对数据进行校验，并显示确认信息。确认信息包含报文类型、本端时序和对端时序。报文类型包括接收成功后通知对方继续发送的等待接收文件信息、多次解码错后通知对方显示校准图像的的申请校准信息、多次校准错误后通知对方跳过当前文件的信息、当前分片与已接收文件数据不一致时通知对方文件重传的信息、文件接收完成时通知对方接收完成的信息。确认信息包含的内容及格式如表2所示。

表2 接收端确认信息的内容格式

字段号	字段名	字节数	说明
1	报文类型	1	0: 未定义; 1: 接收完成; 2: 文件重传; 3: 申请校正; 4: 等待接收文件; 5: 跳过当前文件;
2	本端时序	4	本端发送本报文时的时序，毫秒级
3	对端时序	4	本端收到对端上次报文的时序，毫秒级

其中，有效报文类型初步定义了五种，如：

“1：接收完成”：表示待传输数据拆分的分片均已传输完毕，即文件接收完成信息；

“2：文件重传”：表示当前分片与已接收文件数据不一致时通知发送方重传文件的信息；

“3：申请校正”：表示多次解码错后通知发送方显示校准图像的的申请校准信息；

“4：等待接收文件”：表示当前分片接收成功后通知发送方继续发送后续分片的信息，即接收成功后通知对方继续发送的等待接收文件信息；

“5：跳过当前文件”：表示多次校准错误后通知发送方跳过当前文件，发送下一个文件的信息。

(4) 发送端对确认信息的响应流程

1) 发送端通过摄像头拍摄接收端显示的确认信息图像;

2) 发送端解析确认图像包含的信息,如果是重复或错误二维码,则返回步骤1)重新扫描;如果是成功接收,要求继续发送的信息(即继续发送的接收成功信息,对应上表中的“4:等待接收文件”),则在副屏幕上显示下一个待传输的图像码图片;如果是要求本文件重新发送,则重新发送本文件;如果是申请重新校准(解码方重新生成单应矩阵需要编码方显示棋盘格图片),则发送端显示校准图像,即在副屏幕上显示棋盘格图片;如果申请跳过本次发送文件,则跳过,传输下一个文件。

4. 异常处理机制

考虑到在传输过程中,由于各种因素干扰,可能会出现错误。为了判断接收数据是否正确,同时为了应对可能出现的情况,我们设置了错误检测和处理机制。

(1) 设置循环冗余校验码(cyclic redundancy check)简称CRC(循环码),即编码图像中报文头、数据头和数据区均有对应的CRC---如表1报文头内的各个CRC,每解码一部分则检查CRC是否一致,若发生错误则停止解码。

(2) 校准程序,当文件单个分片(即待传输数据拆分的某个分片,下同)的CRC校验始终错误,会触发校准程序,重新计算单应矩阵。

(3) 跳文件,当文件单个分片(即待传输数据拆分的某个分片)接收错误并且校准之后继续错误,会要求发送方跳过这个文件(即该待传输数据),发送下一个文件(即下一个待传输数据)。

(4) 文件重传,当解码得到的数据与当前接收文件不一致时,会要求发送方重新发送当前文件。

(5) 等待接收文件,当文件单个分片解码成功且被接收后,接收方会要求发送方继续发送下一个单个分片所对应的图像码。

三、本技术与主流方案的对比分析

光盘摆渡机:利用光盘实现数据传输,可实现完全的物理隔离,但无法实现数据的高速传输,无法满足网间数据实时同步的业务需求。数据拷贝由人工完成,数据安全性难以审查,数据无法追溯,且光盘消耗严重,性价比低。

网闸:数据可自动传输,业务应用方便,但无法实现物理隔离,提供协议代理的网闸甚至无法实现网络隔离,依赖配套的安全检测系统确保网络安全。

单向光闸:数据可自动单向传输且传输速度快,但不能实现物理隔离,其物理链路易被利用,存在安全隐患。

二维码摆渡系统:数据可自动单向传输且可实现物

理隔离,但传输速度很低,提高传输速度需要高昂的硬件成本。

本技术方案:数据可自动单向传输且确保物理隔离,传输速度快,可防窃取防伪装,安全可控。

四、总结与展望

本文通过自主设计的图像编码方式生成新的图像码进行信息传输,相比于基于二维码的数据传输方案,大大提高了单次传输量和传输速度,目前单张传输量达到10934个字节,除去报文头和数据头,单幅图像可包含文件数据为10561个字节,数据容量为传统二维码的3.57倍。

使用自主研发的编解码算法处理数据图像,既提高了单幅图像的编码量,又能保证数据不被窃取、泄露。使用机器学习算法识别编码内容,保证了解码速度和准确性,可在提高传输速度的同时缓解高昂的硬件成本。

基于本文图像编码方式设计的技术方案能够在物理隔离条件下实现数据跨网近实时传输,用于解决国家党政军等职能部门、重要企事业单位的内网和外网数据交换安全性低、效率差的问题。

参考文献:

- [1]王秀和,杨明.计算机网络安全技术浅析[J].中国教育技术装备,2007, No.122(05): 49-50+53.
- [2]邓智群,刘福,慕德俊等.网络隔离体系结构研究[J].计算机应用研究,2005(05): 219-221.
- [3]崔洪亮.数据光盘摆渡装置设计及其控制系统研究[D].哈尔滨工程大学,2016.
- [4]蒲天银.安全隔离网闸技术发展探讨[J].计算机时代,2006(06): 18-19.
- [5]万月亮,朱贺军,刘宏志等.基于光闸的单向传输系统可靠性研究[J].信息网络安全,2010, No.120(12): 25-27.
- [6]宗晓宇.基于计算机视觉的非接触式数据传输方法研究[D].西安科技大学,2018.
- [7]朱珺,关广东.基于二维码的跨域信息安全交换系统设计[J].电子产品可靠性与环境试验,2021, 39(03): 19-23.
- [8]陈彦如,李秋香,宫月.物理隔离环境下基于QR码的数据安全交换系统的研究与实现[C]//公安部第一研究所.2020中国网络安全等级保护和关键信息基础设施保护大会论文集.[出版者不详],2020: 5.DOI: 10.26914/c.cnkihy.2020.064816.
- [9]杨军,刘艳,杜彦蕊.关于二维码的研究和应用[J].应用科技,2002(11): 11-13.
- [10]王杨.二维码传播信息的应用及分析[D].山西大学,2013.
- [11]王政,胡志雄.基于张正友标定算法的内参数线性与非线性解算[J].郑州师范教育,2013, 2(02): 63-66.