基于红外传感的电子通信信息传输自动加密系统

祁玉婷
武汉交通职业学院　湖北武汉　430065

摘　要：随着信息技术的快速发展，电子通信的信息安全问题愈发突出。为了解决信息传输中的安全隐患，提出了一种基于红外传感技术的自动加密系统。系统利用红外传感器进行信息传输，结合数据加密算法，实现对通信信息的实时加密与自动解密，保障信息传输的安全性。介绍红外传感技术的原理及其在通信中的应用优势，探讨系统的架构设计与实现过程，分析系统在实际应用中的安全性与可靠性。展示该系统在不同应用场景中的实际效果，展望该技术的发展前景。

关键词：红外传感；电子通信；加密系统；自动加密；信息安全

引言

信息传输过程中的安全性问题日益凸显。黑客攻击、信息窃取、数据篡改等威胁层出不穷，给个人隐私、企业机密和国家安全带来严峻挑战。保障信息在传输过程中的机密性、完整性和安全性，已成为当前电子通信领域的重要研究课题。

红外传感技术作为一种成熟的无线通信技术，凭借其传输速率快、抗干扰能力强、定向传输等优势，在众多领域得到广泛应用。与其他无线通信技术相比，红外传感器的低功耗、便捷性和定向传输特性，让其在短距离保密通信方面具有独特的应用前景。随着信息加密技术的不断发展，将红外传感技术与自动加密系统相结合，能够大大提高信息传输的安全性[1]。

自动加密系统是应对电子通信安全挑战的有效途径之一，自动化的加密与解密流程，能有效避免人为操作中的安全漏洞，同时提高通信效率。设计并实现基于红外传感的自动加密系统，具有重要的理论与实践意义。

一、红外传感技术概述

（一）红外传感器的工作原理

红外传感器是一种利用红外线来检测和传输信息的装置，基于物体辐射的红外波长来感知周围环境的变化。其工作原理依赖于热辐射特性，红外传感器能够通过接收和发射红外光，探测物体的热辐射信号并将其转换为电信号。这种传感器被广泛应用于非接触式探测和短距离通信领域。红外传感器的核心在于其能量的传递过程，当物体温度高于绝对零度时，它会以红外线的形式向外辐射能量，传感器则通过接收这些信号来获取数据。

（二）红外通信技术在电子传输中的应用

红外通信发送器发出红外光，接收器接受这些光信号后，将其转换成电子信号进行处理。这种方式广泛用于遥控器、智能设备以及安全性要求较高的短距离通信场景中。在数据传输时，红外通信依赖的是光的直线传播，无需复杂的天线设计，这让红外通信设备体积小、成本低，适用于大量的消费级电子设备。红外传感技术在近距离、定向传输领域的优势极为突出，能够有效减少外界干扰，让其特别适合用于需要较高保密性的数据传输场景。

（三）红外传感技术的优势与限制

红外线的直线传播特性使得通信过程中很难被外界拦截，具备更好的安全性。红外通信的低功耗和高效性让它在移动设备、物联网设备中得到了广泛应用。红外线频段资源丰富，不易受到无线电频率的干扰，使其在复杂环境中仍能保持稳定通信。由于红外线的直线传播特性，它对传输距离和视距有较高的要求，传输过程容易受到物理障碍物的阻挡。红外通信对光线条件也有一定的依赖，强烈的环境光可能会干扰其传输质量[2]。

二、电子通信信息传输技术分析

（一）现代电子通信系统的基本结构

发送器的主要功能是将数据信号编码并转换成适合传输的形式，通过通信信道进行传递。通信信道能够是

作者简介：祁玉婷（1987.8–），女，汉族，甘肃白银，本科，讲师，研究方向：电子信息技术。

有线的，如光纤和电缆，也可以是无线的，如电磁波或红外线。接收器的任务是接收来自信道的数据并进行解码，还原出发送的原始信息。在这个过程中，信号处理单元负责数据的压缩、调制、纠错等技术操作，保障数据传输的效率和准确性。

（二）信息传输中的主要安全隐患

随着通信技术的广泛应用，数据在传输过程中容易遭受未经授权的拦截、篡改和伪造等攻击。黑客利用中间人攻击等手段拦截数据传输，窃取或篡改敏感信息。信道中的噪声干扰也会导致数据丢失或误传。这些问题让电子通信系统在保障信息安全性方面面临严峻的挑战。

（三）常见的信息加密技术

常见的信息加密技术主要包括对称加密和非对称加密两种方式。对称加密是指在加密和解密过程中使用同一个密钥，该方法的加密速度较快，适用于大规模的数据传输。常见的对称加密算法包括DES、AES等。对称加密的一个主要问题在于密钥的分发与管理，所有通信双方都必须使用同一个密钥，如果密钥被泄露，整个通信的安全性将受到威胁。

发送方使用接收方的公钥对信息进行加密，只有接收方使用自己的私钥解密数据。这种加密方式解决了密钥分发问题，提升了安全性，但由于非对称加密的运算复杂性较高，其加密速度相比对称加密要慢，因此多用于密钥交换等安全敏感的场景。常见的非对称加密算法包括RSA和ECC[3]。

在信息传输的过程中，红外传感技术以其高定向性、低功耗、抗干扰能力强等优势，成为某些特定应用场景中保障通信安全的有效工具。红外传感器用于短距离的信息传输，通信过程中很难被外部无线设备干扰和截取，极大地提高了数据传输的保密性。在医疗设备中，红外通信常被用于短距离的设备互联与数据传输，防止重要病患信息在无线传输过程中被拦截或泄露。红外传感技术还应用于军事通信中，利用其隐蔽性和高安全性，在近距离内实现机密信息的安全传输。

（四）信息传输中的红外传感应用实例

许多家用电器，如电视、空调等，采用红外传感器实现遥控信号的传输。虽然这类应用场景的通信距离短，但其高定向性和安全性为防止误操作和信息干扰提供了保障。在银行自动取款机（ATM）中，红外传感技术被用于银行卡插入、交易信息确认等过程，保障用户敏感信息的安全传输。

三、自动加密系统设计

（一）系统总体架构设计

基于红外传感技术的自动加密系统主要由几大核心模块构成，包括红外传感器模块、数据传输模块、加密模块，以及系统集成和通信流程。这些模块相互配合，实现从信息采集、加密、传输到解密的完整流程，保障信息传输的安全性。

整个系统的核心任务是实现自动化的加密与解密流程，保证信息传输的安全性和可靠性。系统架构主要分为数据采集层、加密处理层和传输解密层。在数据采集层，红外传感器负责接收和检测信息，并将其转换为电子信号。加密处理层则是系统的安全核心，自动加密算法对数据进行加密，保障在传输过程中不被窃取或篡改。传输解密层接收到加密信息后，通过解密算法恢复原始数据，完成通信。

红外传感器通过探测环境中的红外辐射信号，将其转换为电信号，这些电信号携带的数据被传送到加密模块进行处理。在设计时，红外传感器需要具备高精度和稳定性，保证采集信息的准确性。红外传感器的定向传输特性需要优化，让其在特定的方向上发送或接收信号，提升信息传输的保密性。

红外通信的特点是低功耗和高定向性，适用于短距离的安全通信。该模块的核心在于怎样稳定且高效地传输加密数据。由于红外线传播的直线性特点，设计时必须确保发送和接收器之间的视线无障碍。传输过程中，系统会对红外信号进行调制，适应不同的通信环境。为了防止外部干扰，传输信号结合动态频率调整和自适应调制技术，保障信息在复杂的物理环境中依然能够稳定传输。

为了提高安全性，系统采用了对称加密和非对称加密的结合方式。在信息的初次加密时，系统会使用非对称加密算法（如RSA）生成密钥，保证通信双方的身份认证和密钥交换的安全性。一旦双方的身份确认完成，系统将使用对称加密算法（如AES）对实际传输的数据进行加密。对称加密具有运算速度快、加密效率高的优点，适合大规模数据的实时加密传输。非对称加密则在保障密钥安全性方面起到了至关重要的作用[4]。

（二）自动加密算法与技术实现

该过程完全自动化，不需要人工干预。在系统中，红外传感器接收到数据信号后，数据会被迅速传送到加密模块。加密模块根据事先设定的密钥和加密算法，自

动对数据进行加密处理。整个加密流程在极短的时间内完成，保障数据能够即时传输，避免延迟。

在接收端，解密模块负责将接收到的加密信息还原为原始数据。系统会对发送过来的加密数据进行身份验证，确认数据的完整性和传输来源的合法性。解密模块使用与加密相对应的解密算法和密钥，将数据解码。非对称密钥技术保证了密钥的私密性，只有合法接收者才能解密成功，防止数据被第三方恶意解读。

（三）系统集成与通信流程

加密系统与传输系统的结合是实现数据安全传输的关键。在数据从红外传感器采集后，立即被送往加密模块，进行加密处理。加密完成后，数据通过红外传感系统进行传输，在接收端，数据解密后还原为可用信息。这个过程中，系统根据精确的时间同步和信号调度，保障数据能够在规定时间内完成加密、传输和解密。自动化的流程设计减少了人为干预的风险，保证了信息的实时性和安全性。

红外线的定向传播特性保证了数据传输的隐蔽性，加密技术则提供了数据的机密性和完整性。两者相辅相成，实现了高效、保密的信息传输。自动加密技术与红外传感的结合，系统能够适应复杂的环境，满足高安全性需求，在军事、金融和医疗等领域的应用中，具有极高的实用价值。

四、应用场景与系统实现

（一）典型应用场景

红外传感技术因其定向传播特性和较强的抗干扰能力，非常适合应用于短距离、高保密要求的战场通信。例如，士兵之间的战术指令传输或武器系统之间的通信，采用红外自动加密系统能够有效防止外部监听和信息泄露。红外通信的定向性使得信号传播路径隐蔽，不易被敌方截获，加密算法确保了信息即便被拦截，也难以破解。

公司内部的财务数据、商业合同等敏感信息，要通过安全的渠道传输。利用红外加密系统，有效避免无线网络中常见的中间人攻击、数据窃听等问题。自动化的加密过程简化了员工操作，降低了人为失误造成的信息泄露风险。该系统还能用于企业内部的局域网通信，保障商业机密信息只能在特定的范围内传输和接收，提升安全性。

随着数字医疗的普及，患者的隐私数据，如病历、诊断报告等，需要在医疗设备之间或医院内部网络中安全传输。由于红外传感器具备低功耗和短距离传输的优势，适合用于医疗设备之间的无线连接。该系统通过自动加密技术，保障患者的敏感信息在传输过程中不会被外部截获或篡改，提高医疗数据的安全性和隐私保护。

（二）系统在实际应用中的性能评估

系统的响应速度在多场景应用中表现优越。红外传感器的即时数据采集能力，结合高效的加密算法，让信息在接收后能够迅速完成加密处理，立即传输到接收端。整个流程几乎不产生延迟，适用于需要实时通信的应用场景，例如军事战术指令的传递或金融交易系统的内部信息流转。

非对称加密的使用保证了密钥的安全分发，对称加密则保证了数据传输的高效性。即便在复杂环境下，系统也能够抵御常见的攻击手段，如中间人攻击、数据篡改等。对于敏感数据的传输，系统会自动调整加密等级，应对不同场景下的安全需求。

结论

探讨了基于红外传感的自动加密系统的架构设计、加密技术和实际应用场景。红外传感器的高定向性和加密算法的结合，有效提升信息传输的安全性和保密性，在军事、商业和医疗数据传输中表现优异。该系统的高响应速度和强加密性保障了信息在各种应用场景中的实时安全传输。

参考文献

[1] 刘妍萍.基于红外传感的电子通信信息传输自动加密系统[J].自动化与仪器仪表，2022，(04)：93-97.

[2] 于小强，杨晖，杨海马，等.基于红外通信的无线传感节点在漏缆检测中的应用[J].传感技术学报，2014，27(01)：149-152.

[3] 郭明伟.新一代通信网络中的高效电子信息工程技术研究与应用[J].数字通信世界，2024，(08)：37-39.

[4] 高巨.通信电子线路专业课程设计的教学探索——以无人集群应急通信虚拟仿真实验为例[J].科技资讯，2024，22(14)：215-219.