 DOI: https://doi.org/10.12345/gcjsygl.v5i17.8320

Research on Information Processing and Confidentiality Based on Security Monitoring

Bin Ji

The 718th Research Institute of China State Shipbuilding Corporation Limited, Handan, Hebei, 056027, China

Abstract

In order to further meet people's needs for social security, we need to apply modern science and technology to effectively curb the occurrence of such theft. In this context, security technology has rapidly developed into an important means of anti-theft. At the same time, the secure transmission of image information and encryption technology are the main direction of its future development.

Keywords

security monitoring; information processing; confidentiality research

基于安防监控的信息处理及保密研究

吉彬

中国船舶重工集团公司第七一八研究所，中国·河北 邯郸 056027

摘要

为了进一步满足人们对于社会治安方面的需求，需要应用现代化科学技术来有效地遏制这类盗窃事件的发生。在这样的背景之下，安防技术迅速发展成为重要的防盗窃手段，同时基于图像信息的安全传输以及加密技术更是其未来发展的主要方向。

关键词

安防监控；信息处理；保密研究

1 引言

当前中国盗窃犯罪案件的发生较为频繁，同时也呈现出逐步上升的趋势，这对于中国社会治安方面的影响无疑是极为严重的。随着社会各界对于治安问题重视程度的不断增加，中国政府对于该方面也采取了很多措施帮助遏制这类恶性事件的发生，其中安防技术的出现无疑起到了较好的作用。其中监控信息的处理及保密技术即是安防监控技术的重要内容，其在当前的应用中也得到了进一步的推广。

2 基于安防监控的信息处理及保密研究现状及意义

2.1 研究现状及发展方向

据调查可知，由于一些不法分子往往通过破解安防监控图像信息来传输虚假图像，从而迷惑警方人员，继续进行作案，这也对社会的稳定造成了很大的威胁。因而对于图像数据的保护越来越重视，安防监控中的信息传输处理及保密技术也得到了快速的发展。当前安防监控产品也是多种多样，诸如社区防盗、汽车防盗等的发展态势良好，同时已有的单片机信息数据处理技术也有了快速的发展。但该产品由于未应用加密技术，在使用的过程中存在着很大的隐患。随着信息技术的快速发展以及通信保密的广泛应用，安防监控技术未来的发展中将重点基于图像信息的安全传输以及加密技术进行研究，由此提高其保密效果。

2.2 关于安防监控信息处理及保密研究的意义

论文中主要就安防监控信息处理及保密技术进行研究，在此过程中基于信息采集及加密技术进行大规模可编程逻辑器件的研究，并将之广泛地应用于通信、工业等系统之中。总体来看，这方面的研究对于图像信息的加密以及社会治安保障都有着很大的帮助，同时也能最大化地满足人们对于社会稳定方面的要求，以此来保障经济的快速发展[1]。

3 数字图像加密技术简要分析

3.1 密码技术

就目前而言，密码技术是信息安全保障的重要方式，而密码技术的发展历程较长，经过百余年的发展，其应用范围始终在不断扩大，同时也开始应用于军事领域。密码技术是一项较为复杂的综合性技术，其有效地将计算机科学、电子

【作者简介】吉彬（1982-），男，中国河北邯郸人，本科，工程师，从事设备维修管理研究。

通信等技术进行融合应用，从而提高了信息的机密性。不仅如此，密码技术的使用也能防止信息被不法分子篡改或是伪造，因而信息的准确性方面也得到了一定的保障。对于密码技术的实际应用而言，相关加密算法的确十分有必要。当前为了防止密码分析往往采取以下的机制：首先是强壮的加密算法，这类加密算法与密钥的位数密切相关，使用穷举法才能最终解密，因而密钥越长则保密性能越好。除此之外，保护关键密钥的采取也是较为常见，在此过程中需要定期的变换密钥，这也是由于这类信息泄露后果严重所导致的。随着密码技术的不断发展，现代密码技术也进行了划分，主要分为对称以及非对称密码技术两种。对称密码体制中加密以及解密的密钥是相同的，其算法速度较快，应用范围也比较广。而非对称密钥则包含公共密钥以及专用密钥，一般地，公共密钥可以公布，这也是保障专用密钥安全的重要举措，而用公共密钥加密的信息必须使用专用密钥进行解密，这方面的算法也较为复杂。

3.2 数字图像加密技术的分类简要分析

就目前而言，数字图像加密方法多种多样，而根据其加密方式的不同也可以进行一定的划分，诸如基于现代密码体制的加密方法、基于混沌系统的加密方法以及基于压缩编码技术的加密方法等。首先基于现代密码体制的加密方法为数字信息的安全保密提供了基础，也帮助一些经典算法取得了成功。据分析可知，密码体制的加密方法契合于图像文件的加密，经过诸多学者长期的研究也开始将椭圆曲线应用于图像加密之中。而基于混沌系统的加密方法则是由 Matthews 提出的，这方面数据加密方法较为重要，也是近些年来发展起来的加密技术，其可以将加密的图像信息按照某种编码方式来进行应用，最终利用混沌信号来对其图像技术进行加密，其他类型的数字加密技术就不进行具体的介绍分析了。

3.3 基于 DES 算法的图像加密方法

DES 是一种数据加密标准，同时也是由其他国家学者所提出的数据加密方法，该加密方法也被美国用于加密政府及商业的一些非要害信息。经分析可知，DES 属于对称密码体制，因而其应用过程中加解密的速度较快，安全性也比较高。当前 DES 算法也被广泛地应用于加油站等领域，用以加强一些关键数据的保密性能。此外，金融交易数据包的校验以及 PIN 的加密传输等也都应用了 DES 算法。DES 算法的基本思想即是在 64 比特密钥的控制下，将其每 64 个比特分为一组，从而按照分组进行加密操作。DES 算法运行中，首先是利用初始置换表来进行换位处理，并在密钥的控制下进行 16 论迭代处理，并经过交换来得到 64 比特密文。一般的，DES 密钥为 64 位长，而用户往往是提供 56 位，剩余的 8 位则需要根据算法进行提供。其中 16 个阶段中各个阶段都将使用 48 位密钥，此密钥最初也是由 64 位密钥派生而来的 [2]。

3.4 改进 DES 后的图像加密算法简要分析

基于 DES 算法的图像加密需要考虑的内容很多，首先是要解决如何将图像色彩的二维数据转化为一维数据，在此过程中也需要对一维数据进行分组加密。经过该加密操作后，其图像处理也更为保密，实际应用的效果也比较好。初始置换表 IP 表改用 Fibonacci 置换表 FIP 表，而其余算法则保持不变，由此便能得到新的加密方法。在此过程中，其具体的加密算法步骤如下，首先需要构架基于 Fibonacci 置换表 FIP 的新 DES 模块，之后输入之前的图像信息，并将之向一维数据进行转化。转化之后，输入 64 比特密钥，同时利用改进的 DES 算法来将每 64 比特数据为一组，从而加密所有的图像，并得到加密后的相关数据。最后即是将一维数据转换为二维数据，得到加密后的秘密图像。经过实践分析比较后可知，改进后的 DES 算法保密效果更好，其应用也有效地解决了传统加密方法的不足之处 [3]。

4 静态图像编码于加密的结合简要分析

一般地，由于存储资源和网络宽带的限制，图像数据内容较为庞大，这就需要将其以压缩的形式进行存储或是运输。这就对加密算法提出了严格的要求，加密算法需要抵抗压缩攻击或是直接与压缩过程相结合，由此才能确保图像数据内容的保密性。就目前而言，新一代的静止图像压缩标准，即 JPEG2000 已然发布，其一经推出便得到了广泛的应用，但仍需要在后续的使用中对加密技术理论以及应用的发展提供新的契机。由上述的分析可知，压缩后的图像数据去除了图像的空间或时间相关冗余性，因而其数据可能包含不同类型的信息，这些信息都有必要进行加密处理。

5 结语

论文中就安防监控相关的信息处理及保密技术进行了深入的探讨分析，在此过程中，重点介绍了数字图像加密技术以及 DES 保密技术，在此基础上，进一步深入探究了静态图像编码与加密的结合。总体而言，都是为了有效地提高重要信息的保密性。

参考文献

[1] 田国银,翟桂全,左伟.“互联网+”背景下科研院所保密工作现状与对策研究[J].江苏科技信息,2021,38(20):44-47.

[2] 熊宁.国有企业数字化转型中的网络安全防护与保密管理[J].网络安全技术与应用,2021(7):118-119.

[3] 邱文兰,郑斌,蔡建平.间歇控制实现混沌同步及图像保密通信[J].闽南师范大学学报(自然科学版),2021,34(2):22-28.