Journal of Image and Signal Processing 图像与信号处理, 2019, 8(2), 98-102
Published Online April 2019 in Hans. http://www.hanspub.org/journal/jisp
https://doi.org/10.12677/jisp.2019.82014

Hans汉斯

Image Encryption Algorithm Based on the Hardware Platform

Xiaoqiang Zhang[1,2], Hang Yang[3], Xun Wang[1], Wei Zeng[3]

[1]School of Information and Control Engineering, China University of Mining and Technology, Xuzhou Jiangsu
[2]School of Electrical and Power Engineering, China University of Mining and Technology, Xuzhou Jiangsu
[3]Xuzhou Key Laboratory of Artificial Intelligence and Big Data, Xuzhou Jiangsu
Email: grayqiang@163.com

Received: Apr. 3rd, 2019; accepted: Apr. 14th, 2019; published: Apr. 28th, 2019

Abstract

The image is an important carrier under the network platform. With the development of the Internet, the image transmission becomes fast and easy. These images always carry a lot of confidential information. In recent years, the image security attracts the attention of scholars at home and abroad. Traditional image encryption is mostly designed based on the software. In recent years, with the development of hardware platforms, DSPs and FPGAs are applied to image encryption for its processing speed, logic computing power and low cost. This paper introduces the technology of image encryption. Meanwhile, this paper mainly describes the image encryption algorithm based on DSP and the image encryption algorithm based on FPGA. Their advantages and disadvantages are also discussed. Finally, we prospect the application prospect of FPGA in the field of image encryption.

Keywords

Information Security, Image Encryption, FPGA, Zu Chongzhi, DSP, Chaos

基于硬件平台的图像加密算法

张晓强[1,2]，杨　航[3]，王　迅[1]，曾　炜[3]

[1]中国矿业大学信息与控制工程学院，江苏　徐州
[2]徐州市人工智能与大数据重点实验室，江苏　徐州
[3]中国矿业大学电气与动力工程学院，江苏　徐州
Email: grayqiang@163.com

收稿日期：2019年4月3日；录用日期：2019年4月14日；发布日期：2019年4月28日

文章引用：张晓强，杨航，王迅，曾炜. 基于硬件平台的图像加密算法[J]. 图像与信号处理, 2019, 8(2): 98-102.
DOI: 10.12677/jisp.2019.82014

摘　要

图像是网络信息传递的一种重要载体。随着互联网的发展，图像的传输也变得更加便捷。然而，这些图像往往携带了一些涉密信息。近年来，网络安全事件的频繁发生，图像内容的安全备受国内外学者的广泛关注。传统的图像加密大都是基于计算机软件而设计的。近年来，随着硬件平台的发展，DSP和FPGA以其处理速度、逻辑运算能力和低成本的特点越来越多地被应用于图像加密领域。综述图像加密的技术，特别是对基于DSP的图像加密算法和基于FPGA的图像加密算法进行了详细描述，并讨论了这两种算法的优缺点。最后，对FPGA在图像加密领域的应用前景进行了展望。

关键词

信息安全，图像加密，FPGA，祖冲之，DSP，混沌

1. 引言

人类通过视觉系统获取大量的信息，图像作为信息传递的一种重要载体，在人类社会的工作生活中扮演着重要的角色。随着近年来网络技术的蓬勃发展，图像的在线传输变得越来越频繁。在这些被频繁传输的图像中，包含了大量的个人隐私、企业机密、国家机密等不能被第三方获取的重要信息。互联网以开放性和共享性著称。然而，由于现阶段网络空间各类不确定因素过多，安全性参差不齐。近年来，随着网络安全事件的不断发生，大量的隐私遭到泄密，对国家安全、国民经济发展和个人利益带来了不同程度的影响。图像安全逐渐得到了社会各界的广泛关注。当前，图像加密算法主要有以下几类：基于混沌的图像加密、基于变换域的图像加密、基于盲源分离的图像加密和基于空间域的像素置乱。

综述了图像加密技术，重点分析了基于硬件的图像加密算法。讨论了基于 DSP 的图像加密算法和基于 FPGA 的图像加密算法的优缺点，并对 FPGA 在图像加密领域的应用前景进行了展望。

2. 图像加密技术综述

自上世纪 90 年代以来，图像加密就受到了世界各地学者的广泛关注。1996 年，第一届信息隐藏领域的学术研讨会在英国剑桥举办。自此，人们开始关注并研究图像安全技术。迄今为止，数十届信息隐藏国际研讨会的成功举办吸引了众多学者的投入到图像安全的研究领域中。普林斯顿、麻省理工等世界名校以及 IBM 等国际大公司也一直致力于图像安全方面的研究[1]。

图像加密的本质就是把待加密的图像进行像素位置的置乱或像素值的改变，使得整幅图像对外呈现出类似于噪声图像的特征，从而达成加密图像不能被第三方识别的目的。目前，人们已提出了多种图像加密算法，按照算法依托的平台不同，可分为：基于软件的图像加密算法和基于硬件的图像加密算法。

2.1. 基于软件的图像加密算法

二十世纪六十年代，美国气象学家 Lorenz 在研究气象问题时提出了著名的 Lorenz 方程；1989 年，英国数学家 Matthews 首次提到了“混沌密码学的概念”，成为首个将混沌理论引入图像安全领域的学者；

1997 年，Fridrich 将混沌系数运用到了图像加密领域[2]。二十世纪九十年代，定向 Hamilton 路径问题被 Adleman 用 DNA 分子解决，这一方案代表着 DNA 计算的开始[3]。Kulsoom 等把像素的高位和地位分开进行 DNA 编码，将 DNA 概念与混沌映射加密算法相结合，开启了新的加密方向。

基于软件的图像加密算法主要可以分为：基于现代密码体制的图像加密算法，基于矩阵变换的图像加密算法，基于混沌的图像加密算法，基于秘密分存的图像加密算法，基于频域的图像加密算法，基于 SCAN 语言的图像加密算法和基于 DNA 编码的图像加密算法[4]。

2.2. 基于硬件的图像加密算法

传统的图像加密多基于计算机，计算机是基于冯诺依曼结构，难以满足数据量大和逻辑运算复杂的加密运算。随着 DSP、FPGA 这些专用硬件设备的发展，特别是 FPGA 对复杂逻辑运算的处理能力，图像加密将会越来越多的在专用硬件设备上实现[5]。

3. 基于 FPGA 的图像加密算法

现场可编程门阵列(Field-Programmable Gate Array, FPGA)是在保留了 GAL、CPLD 等可编程器件优点的基础上，进一步优化而来的产物。FPGA 内部含有大量的乘法器，可用来实现复杂的逻辑运算。近年来，FPGA 由其出色的逻辑运算能力受到了图像加密领域的广泛关注。

祖冲之算法，又称 ZUC 算法，隶属于序列密码，是我国自主设计的加密完整性算法，也是我国第一个成为国际密码标准的密码算法。

祖冲之算法分为三个逻辑层，如图 1 所示。第一层为线性反馈移位寄存器(linear feedback shift register, LFSR)，第二层为比特重组层，第三层为非线性函数层。第一层中含有 16 个逻辑单元，每一个单元包含 31 个比特，这些比特不能完全相同，即不能全为 0 或者全为 1；第二层根据第一层的数据，选取其中的一部分，重新组合成 4 组 32 bit 的数据 X_i；第三层对主要完成对第二层重组的数据进行非线性变换，产生 32 bit 数据流。

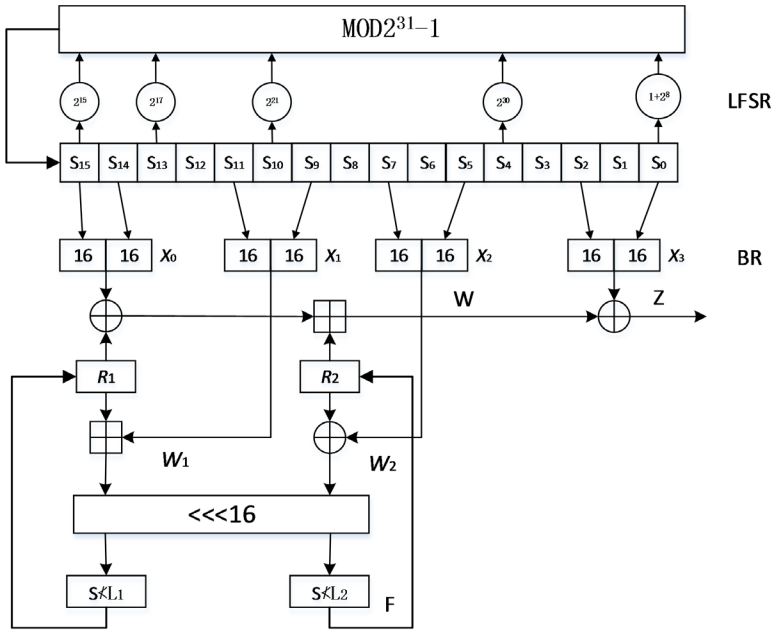

Figure 1. Zu Chong's algorithm
图 1. 祖冲之算法

祖冲之算法是一种基于序列的密码算法，在 FPGA 中实现时只需要占用 618 个寄存器，最高频率可达 124.64 MHz，吞吐量可达 3988.48 Mbps [6]。该算法工作在两种模式，即初始化模式和工作模式，如不更换秘钥，则不需要重复执行初始化模式，可以直接进入工作模式。基于 FPGA 的祖冲之算法，占用的资源较少，工作效率高。

4. 基于 DSP 的图像加密算法

为了适应高速信号处理任务，数字信号处理器(Digital Signal Processor, DSP)逐渐发展起来。DSP 的一大显著特点就是具有零消耗循环控制的专门硬件；DSP 采用哈弗结构，程序和数据分开存储，总线也分为程序存储器的数据总线和地址总线以及数据存储器的数据总线和地址总线。DSP 内部的硬件乘法器(MUL)、累加器(ACC)和算术逻辑单元(ALU)等可以在一个周期内同时运算，具有较高的数据处理速度和效率。

混沌是一种繁复的非线性、非均衡的动力学过程[7]。混沌理论是一种周期与非周期运动相互纠缠，最终通向非周期有序运动的理论[8]。Logistic 映射是一个常用的混沌系统，其数学模型简单，对于所产生的混沌特性和统计特性的分析也较为容易[9]。Logistic 映射的数学模型如下：

$$x_{k+1} = ux_k\left(1-x_k\right), \tag{1}$$

其中，$x_k \in (0,1)$，u 为分岔参数。

在设计图像加密混沌系统时，把加密的明文设置成系统的部分初始条件，把加密的秘钥设置为系统的另一部分初始条件，在经过系统对的多次迭代后，明文和秘钥变得充分混合，取得良好的加密效果。

DSP 基于哈弗结构，DSP 的零消耗循环控制和哈佛式结构使其在完成混沌系统的多次迭代时具有较大的优势，在图像加密领域涌现出了较好的应用前景。混沌加密及解密的原理及其实现过程如图 2 所示，编码后的图像信息以二进制数据流的形式传输，利用 DSP 产生混沌序列与二进制数据流相互作用，得到用于发送的密文，利用 DSP 编写该加密程序执行速度快，加密效果良好，安全性高。

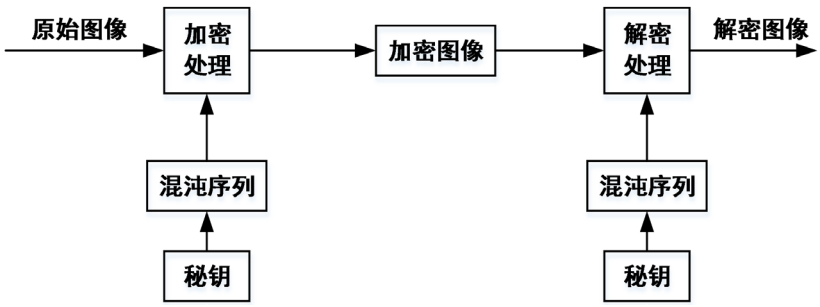

Figure 2. Chaos encryption and decryption process
图 2. 混沌加解密过程

5. 结论

本文重点综述了基于硬件的图像加密算法。详细描述了基于 DSP 的图像加密算法和基于 FPGA 的图像加密算法的加密原理，并讨论了它们的优缺点。1) 基于 DSP 的图像加密算法：DSP 采用哈弗结构，程序和数据分开存储，DSP 可实现一定的并行处理。近年来涌现了大量的 DSP 专用芯片来完成实时图像加密，但 DSP 难以应对较为复杂的逻辑运算；2) 基于 FPGA 的图像加密算法：FPGA 的特点是并行处理，可同时进行多个任务，并且其内部集成锁相环，具有丰富的逻辑资源，可应对视频图像加密对速度和逻辑运算能力的要求。同时，对于图像加密方式的灵活性和图像加密方式的多样性，FPGA 的大量 IP 内核

可出色地满足这些特性。基于 FPGA 的图像加密具有广阔的前景，FPGA 正以其并行性、高效性、维护升级的便捷性越来越广泛地被应用于图像加密。

致　谢

非常感谢国家自然科学基金“大容量高安全的加密域图像可逆水印算法研究”(61501465)和江苏省大学生创新训练项目“基于 LabVIEW 的遥感图像加密系统”(201810290102X)对该文的资助。

参考文献

[1] 颜世银. 基于混沌的图像加密方案研究及实现[D]: [硕士学位论文]. 上海: 华东师范大学, 2008.

[2] Matthews, R. (1989) On the Derivation of a “Chaotic” Encryption Algorithm. *Cryptologia*, **13**, 29-42. https://doi.org/10.1080/0161-118991863745

[3] Zhen, P., Zhao, G., Min, L., *et al.* (2016) Chaos-Based Image Encryption Scheme Combining DNA Coding and Entropy. *Multimedia Tools and Applications*, **75**, 6303-6319. https://doi.org/10.1007/s11042-015-2573-x

[4] 张晓强, 王蒙蒙, 朱贵良. 图像加密算法研究新进展[J]. 计算机工程与科学, 2012, 34(5): 1-5.

[5] Nassar, N., Newhook, R. and Miller, G. (2014) Enhanced Mobile Security Using SIM Encryption. 2014 *International Conference on Collaboration Technologies and Systems* (*CTS*), Minneapolis, 19-23 May 2014, 189-196. https://doi.org/10.1109/cts.2014.6867563

[6] 程海. 基于 FPGA 的图像加密关键技术研究[D]: [博士学位论文]. 哈尔滨: 黑龙江大学, 2015.

[7] 黄璐. 图像的混沌置乱算法研究[D]: [硕士学位论文]. 长沙: 长沙理工大学, 2011.

[8] Liu, Y., Wang, J., Fan, J., *et al.* (2016) Image Encryption Algorithm Based on Chaotic System and Dynamic S-Boxes Composed of DNA Sequences. *Multimedia Tools and Applications*, **75**, 4363-4382. https://doi.org/10.1007/s11042-015-2479-7

[9] Hua, Z.Y., Zhou, Y.C., Pun, C.M., *et al.* (2015) 2D Sine Logistic Modulation Map for Image Encryption. *Information Science*, **297**, 80-94. https://doi.org/10.1016/j.ins.2014.11.018