一种虚拟光学数据加密的系统实现

张 鹏[1],彭 翔[1,2],牛憨笨[2]
(1. 天津大学精密测试技术及仪器国家重点实验室,天津 300072;
2. 深圳大学光电子学研究所,教育部光电子器件与系统重点实验室,广东深圳 518060)

摘 要: 本文在虚拟光学数据加密理论模型的基础上,研究一种并行电子系统实现方法. 该系统利用 TMS320C6701 浮点 DSP(Digital Signal Processor)实现具有多重锁、多重密钥的高密级多媒体数据加密系统. 该系统具有安全性高、加/解密速度快、实时性好、适用范围宽等优点,可用于多种媒体信息如文本、图像、语音、视频等的加/解密.

关键词: 虚拟光学; 加/解密; 数字信号处理器; 并行处理; 软件流水
中图分类号: TN918 **文献标识码**: A **文章编号**: 0372-2112 (2004) 10-1585-04

An Implementation Scheme of Virtual-Optics Based Data Encryption System

ZHANG Peng[1], PENG Xiang[1,2], NIU Han-ben[2]
(1. *National Laboratory of Precision Measurement Technology and Instrumentation, Tianjin University, Tianjin* 300072, *China*;
2. *Institute of Optoelectronics, Shenzhen University, Key Laboratory of Optoelectronics Devices and Systems of Education Ministry, Shenzhen* 518060, *China*)

Abstract: In this article, we investigate an implementation scheme of virtual-optics based data encryption system. With such a scheme, we make use of a high performance floating-point Digital Signal Processor (DSP) to accomplish a design of multiple-locks and multiple-keys multimedia information hiding system. This scheme balances the advantages of higher security strength in the methodology of optical data processor and the high flexibility in the methodology of electronic data processor. The scheme reported in this article can be applied to the data encryption for various digital media such as text, image, or even audio signal.

Key words: virtual-optics; encryption/decryption; DSP; parallel processing; software pipeline

1 引言

进入信息时代后,信息安全问题成为人们关注的焦点. 数据加密技术被广泛的应用于商业保密、军事通讯等许多重要领域中. 近来,基于光学信息处理的多维数据加/解密方法作为一种新的"非数学"数据加密技术因其具有实时的数据传递速度、密级高、密钥设计灵活且自由度大等优点,已经成为研究的又一热点[1-3]. 在虚拟光学信息加密系统(EVOIS)的理论模型[4,5]的基础上,本文使用 TMS320C6701 DSP 芯片完成了该信息加密系统的硬件和软件实现. 这种硬件和软件实现有效的结合了电子数据加密处理器和光学数据加密处理器各自的主要优点,利用电子手段(并行硬件、并行算法)仿真光学数据处理的过程. 利用数字仿真的光学过程中的传播规律和结构的几何参数作为密钥,通过设计多重"锁"和多重"密钥"实现高密级的数据加密. 实验结果表明,此系统安全级别高、加/解密速度快、抗外界干扰性能强、可实时进行图像及语音的加/解密工作.

2 基于虚拟光学的信息隐藏系统理论模型

考虑一个加入了随机模板(用于模拟随机光场)的单透镜光学成像系统,如图 1 所示.

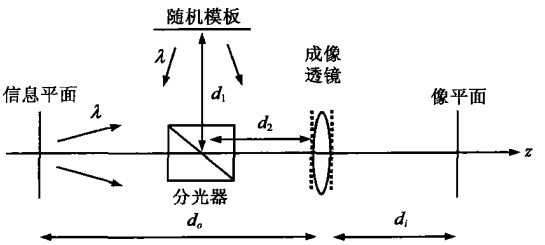

图 1 模型结构示意图

图中,d_0 是物平面(信息平面)到成像透镜前表面的距离,d_i 是透镜后表面到像平面的距离. 物平面,透镜前表面,后表面以及像平面的复振幅分布分别表示为 $U_0(x_0, y_0)$, $U_{L1}(\xi, \eta)$, $U_{L2}(\xi, \eta)$ 和 $U_i(x_i, y_i)$. 假定信息平面和随机模板由相同选定波长的相干光照明,且此成像系统中所涉及的衍射都满足菲涅尔近似条件. 根据傅里叶光学[6],虚拟光波从物平面到透镜前表面的传播过程可用菲涅尔衍射变换来描述. 虚拟光波从透镜后表面到像平面的传播过程也可用菲涅尔衍射变换来描述.

我们要在数字域实现上述透镜成像的过程并利用它进行

收稿日期:2003-02-12;修回日期:2004-08-10
基金项目:国家自然科学基金(No. 60275012);中科院模式识别国家重点实验室开放课题基金

信息加密,需要对 $U_0(x_0, y_0)$ 进行 $N \times N$ 的采样,沿 x_0 和 y_0 方向的采样间隔分别为 Δx_0 和 Δy_0,这样 x_0 和 y_0 可以用 $k\Delta x_0$ 和 $l\Delta y_0$ 替换,其中 k, l 是 0 到 $N-1$ 之间的整数. 同理,ξ 和 η 可以用 $m\Delta\xi$ 和 $m\Delta\eta$ 替换;空间频率 f_X 和 f_Y 用 $m\Delta\xi/\lambda d_0$ 和 $n\Delta\eta/\lambda d_0$ 替换. 离散化过程可以用下面的公式表示,

$$x_0 = k\Delta x_0, y_0 = l\Delta y_0 \qquad k, l = 0, 1, \cdots N-1 \tag{1}$$

$$\xi = m\Delta\xi, \eta = n\Delta\eta \qquad m, n = 0, 1, \cdots N-1 \tag{2}$$

$$f_X = m\Delta f_X = m\frac{\Delta\xi}{\lambda d_0}, f_Y = n\Delta f_Y = n\frac{\Delta\eta}{\lambda d_0} \qquad m, n = 0, 1, \cdots N-1 \tag{3}$$

根据 Shannon 采样定理,可以得到

$$\Delta x_0 = \frac{1}{N\Delta f_x} = \frac{\lambda d_0}{N\Delta\xi}, \Delta y_0 = \frac{1}{N\Delta f_y} = \frac{\lambda d_0}{N\Delta\eta} \tag{4}$$

根据式(1)~(4)可以得到菲涅尔变换的离散表达形式,称为离散菲涅尔变换,简记为 DFD(Discrete Fresnel Diffraction),其中信息平面 $U_0(k, l)$ 的 DFD 如式(5)所示

$$\begin{aligned} U_{L1}(m, n) &= \mathrm{DFD}[U_0(k, l); \lambda, d_0] \\ &= \frac{1}{j\lambda d_0}\exp\left[j\frac{\pi}{\lambda d_0}(m^2\Delta\xi^2 + n^2\Delta\eta^2)\right] \\ &\cdot \sum_{k=0}^{N-1}\sum_{l=0}^{N-1} U_0(k, l)\exp\left[j\frac{\pi}{\lambda d_0}(k^2\Delta x_0^2 + l^2\Delta y_0^2)\right] \\ &\cdot \exp\left[-j2\pi\left(\frac{km}{N} + \frac{ln}{N}\right)\right] \end{aligned} \tag{5}$$

其中 λ 为光波波长. 由上式可以看出离散菲涅尔变换(DFD)的计算可由信息平面与二次因子 $\exp[j\frac{\pi}{\lambda d_0}(k^2\Delta x_0^2 + l^2\Delta y_0^2)]$ 之积的离散傅里叶变换(DFT)实现. 因此可运用快速傅里叶变换(FFT)来计算式中的离散傅里叶变换以提高运算速度.

另外,透镜的复振幅透过率函数也要进行采样,得到其离散形式

$$t(m, n, f) = \exp\left[-j\frac{K}{2f}(m^2\Delta\xi^2 + n^2\Delta\eta^2)\right] \tag{6}$$

式中 $m, n = 0, 1, \cdots N-1$, f 为透镜焦距, K 为波数且 $K = \frac{2\pi}{\lambda}$

在加密过程中,我们用离散菲涅尔变换(DFD)计算信息平面(U_0 用表示)和随机模板(用 U_M 表示)到透镜前表面的衍射,衍射距离分别为 d_0 和 d,其中 $d = d_1 + d_2$. 它们在透镜前表面的菲涅尔衍射图案将发生干涉,得到干涉图,干涉图又经透镜的复振幅透过率函数的转换到达透镜的后表面. 将成像透镜后表面的复振幅分布(用 U_{L2} 表示)作为密文,它可以通过通信链路传送.

下面的方程可以描述上述加密过程[4],

$$\begin{aligned} U_{L2}(m, n) &= \{\mathrm{DFD}[U_0(k, l); \lambda, d_0] \\ &+ \mathrm{DFD}[U_M(k, l); \lambda, d]\} \times t(m, n; f) \end{aligned} \tag{7}$$

在加密过程中,除了 d_0, f 和 λ 以外,随机模板本身的编码和它到透镜前表面的衍射距离 d 也为设计多维密钥提供了可能的途径,这使得不知道正确钥匙的攻击者很难解密出明文的原信息.

在接收端,合法的用户将被告知解密的方法和正确的密钥,解密过程包括下列步骤:

(1)计算所随机模板密钥(U_M' 用表示)的 DFD 变换;结果乘上透镜的复振幅透过率,得到其在透镜后表面的复振幅分布;

(2)将步骤(1)的结果从密文中减去,结果用 U 表示;

(3)对 U 作衍射距离为 d_i 的 DFD 变换,得到原信息的像,即恢复了加密的信息.

下面的方程可以描述上述解密过程[4],

$$U_i(m, n) = \mathrm{DFD}[U'(k, l); \lambda, d_i(d_0, f)] \tag{8}$$

式中,

$$\begin{aligned} U'(m, n) &= U_{L2}(m, n) - \mathrm{DFD}[U_M'(k, l); \lambda] \\ &\times t(m, n; f) \end{aligned} \tag{9}$$

从解密过程我们可以看出,要想完全解密出原信息,除了随机模板外,至少需要知道三个参数,即 d_0, f, λ.

从上述分析可以看出,此理论模型可以用于图像、文本、以及声音信号的加/解密. 当信号为语音信息时,可以利用软件将信息数据读取到矩阵中,再利用数组操作将它的元素重新排列使之成为一个 $N \times N$ 的矩阵,再将其作为图像矩阵按上述过程处理.

3 虚拟光学数据加密系统的 DSP 实现

上述虚拟光学数据加密理论的实现系统是在一块 TMS320C6701 DSP 芯片上完成的. TMS320C6701 是一种高性能浮点数字信号处理器,工作频率 167MHz,属 TI 的 C6000 系列 DSP,运行速度快,指令周期 6ns,峰值运算能力 1336MIPS,硬件支持 IEEE 格式的 32 比特单精度与 64 比特双精度浮点操作,对于单精度浮点运算可达 1G FLOPS[7].

TMS320C6701 是一种具有高并行度的数字信号处理器. 它的空间并行功能(支持多功能单元的并行操作)和时间并行功能(软件流水线)在对图像做并行处理时也有很好的表现. 这些特点在一定程度上弥补了采用电子处理器仿真光学处理过程所丧失的固有的并行处理的能力.

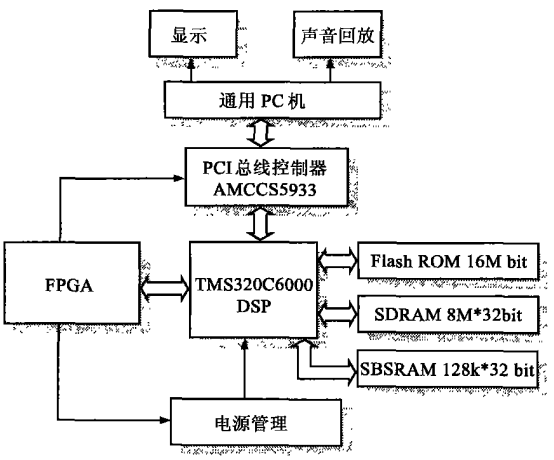

图 2 硬件系统结构图

在系统的实现过程中使用了由 167MHz TMS320C6701 DSP,128K*32 bit SBSRAM,8M*32bit SDRAM,16Mb Flash mem-

ory,AMCC S5933 PCI 总线控制器,XILINX FPGA,电源监测和复位控制电路等构成的 PCI 插卡(DSP 子系统)作为开发工具.使用通用 PC 机控制 DSP 子系统的复位、运行和挂起,DSP 子系统在 PC 机的控制下完成核心加、解密算法. PC 机将数据传送到 DSP 子系统处理,而 DSP 子系统则将处理后得到的结果传递给 PC 机,由 PC 机将处理结果进行显示、打印、回放、网络传输等后续处理.其硬件系统结构如图 2 所示.

4　算法 DSP 实现的详细流程

图 3 和图 4 分别为使用 DSP 实现虚拟光学数据加/解密算法时的详细流程图.

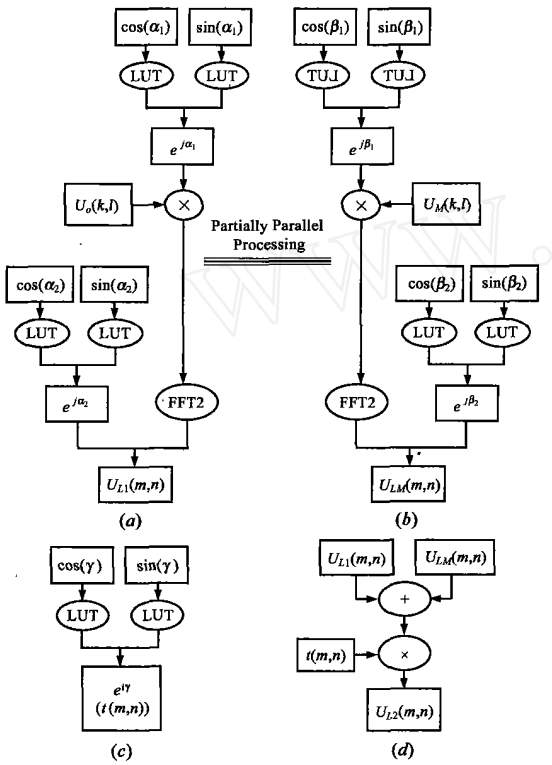

图 3　加密算法设计框图(编码器)

图 3 中出现的中间变量说明如下:

$$\alpha_1=\frac{\pi}{\lambda d_0}(k^2\Delta x_0^2+l^2\Delta y_0^2),\ \alpha_2=\frac{\pi}{\lambda d_0}(m^2\Delta\xi^2+n^2\Delta\eta^2),$$

$$\beta_1=\frac{\pi}{\lambda d}(k^2\Delta x_0^2+l^2\Delta y_0^2),\ \beta_2=\frac{\pi}{\lambda d}(m^2\Delta\xi^2+n^2\Delta\eta^2),$$

$$\gamma=\frac{K}{2f}(m^2\Delta\xi^2+n^2\Delta\eta^2),$$

图 4 中出现的中间变量说明如下:

$$\beta_{1\_key}=\frac{\pi}{\lambda d}(k^2\Delta x_0^2+l^2\Delta y_0^2),\ \beta_{2\_key}=\frac{\pi}{\lambda d}(m^2\Delta\xi^2+n^2\Delta\eta^2),$$

$$\gamma_{key}=\frac{K}{2f}(m^2\Delta\xi^2+n^2\Delta\eta^2),\ \alpha_{1\_key}=\frac{\pi}{\lambda d_{0\_key}}(k^2\Delta x_0'^2+l^2\Delta y_0'^2),$$

$$\alpha_{2\_key}=\frac{\pi}{\lambda d_{0\_key}}(m^2\Delta\xi'^2+n^2\Delta\eta'^2),$$

其中 $\Delta x_0'$、$\Delta y_0'$、$\Delta\xi'$、$\Delta\eta'$ 的尺度根据模拟透镜尺寸要求、采样定理、以及菲涅尔衍射条件确定,并根据解密参数 $\lambda_{\_key}$、$f_{\_key}$、d_{0_key} 作相应变换而来.

在图 3 所示的加密过程中,前述算法中信息平面(U_0)的离散菲涅尔变换(DFD)过程见图 3(a),图 3(b)表示的是随机模板(U_M)的离散菲涅尔变换(DFD).图 3(c)是离散的透镜复振幅透过率函数 $t(m,n)$ 的形成过程.图 3(d)描述的是成像透镜后表面的复振幅分布(U_{L2})即密文的形成过程:

$$U_{L2}(m,n)=\{\mathrm{DFD}[U_0(k,l);\lambda,d_0]+\mathrm{DFD}[U_M(k,l);\lambda,d]\}\times t(m,n)\qquad(10)$$

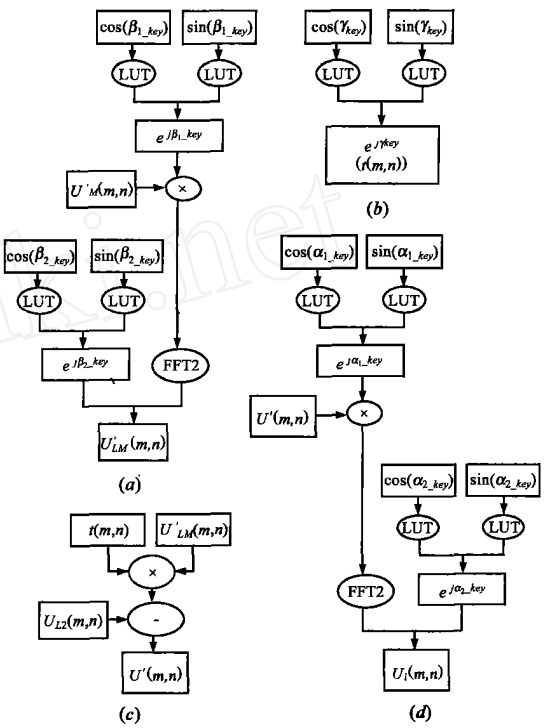

图 4　解密算法设计框图(解码器)

解密过程见图 4,其中图 4(a)所示为随机模板密钥(用 U_M' 表示)的 DFD 变换;图 4(b)为计算透镜的复振幅透过率 $t(m,n)$;图 4(c)所示的过程是将图 4(a)中结果乘上透镜的复振幅透过率 $t(m,n)$,得到其在透镜后表面的复振幅分布;再将其从密文中减去,结果用 U 表示;图 4(d)表示的是对 U' 作衍射距离为 d_i 的 DFD 变换(d_i 是透镜后表面到像平面的距离)的过程,通过这一过程就可得到原信息的像 U_i,即恢复了加密的信息.

为达到实时处理的目的,在进行 DSP 软件开发时,我们使用了大量的并行处理手段和针对 C6000 DSP 芯片的特定软件优化方法.采用了消除冗余循环、循环展开、双字访问两个浮点型变量等多种技术.充分利用 DSP 的并行资源,实现了软件流水,程序性能大大提高.

软件流水[8]是针对算法中最耗时的核心循环来安排循环指令,使循环中的多次迭代并行执行的一种技术.这种技术克服了传统的 CPU 体系结构在程序获取、数据接入和乘法操作方面的瓶颈;在一个时钟周期内,流水线能够调度 8 条平行指令.它的使用使系统中的 DSP 实现了其最佳性能,程序并行度得到进一步提高.

在该算法中最耗时的核心循环为离散菲涅尔变换(DFD).故在进行加密时,通过软件优化,使图像的 DFD 和模板的 DFD(二者不具有相关性)并行处理.在进行解密时,由于两次核心 DFD 算法具有相关性,不能并行处理,所以采取循环展开的方法提高软件性能.我们将执行周期很少的内部循环展开成一个比较大的内部循环,尽可能增加并行执行的指令数,同时对多个像素点进行操作,使 DSP 流水线始终保持充满.这在一定程度上弥补了完全采用电子加密手段而丧失的光学并行处理的优点.但上述并行处理会受到 DSP 本身功能的限制,其峰值(流水线始终充满)也只能达到 8 条指令并行操作,所以只是部分的并行.

从流程图中可以看到正弦三角函数 Sine,余弦三角函数 Cosine 是加/解密算法中大量用到的基本运算,程序的优劣直接影响到加/解密的速度.为提高系统运行速度,采用查找表(LUT)的方法实现这些基本运算.采用查表方法代替数学函数的调用能提高效率,因为表格查找起来执行速度快,,所用代码少,而且省去了函数调用时用来保护现场所需的堆栈空间.

5 系统性能分析

5.1 加/解密效果

为检测用 DSP 实现的基于虚拟光学的信息隐藏系统的各项性能,我们使用了 512 ×512 ×8bits 的灰度图(图 5(a))进行图像信息的加/解密测试,其经系统加密后结果如图 5(b)所示.用于模拟随机光场的随机模板是在 DSP 硬件中利用 TI 的 rand()函数生成的(512 ×512)二维伪随机阵列,如图 5(c)所示.

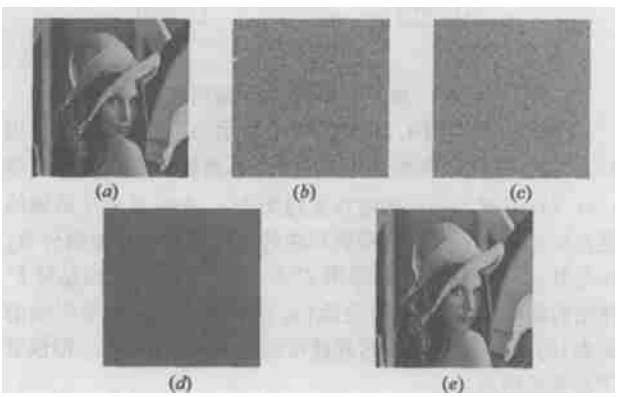

图 5

在解密过程中,如果没有加密时所用的随机模板密钥,即使密钥参数 d_0, f, λ 全部正确,解密仍然不能成功(结果如同是随机的白噪声),如图 5(d)所示.只有当所有的密钥参数正确,又知道随机模板密钥,才可以得到清晰的解密结果,见图 5(e).

5.2 实时性

在 TI 的 CCS(Code Composer Studio)集成开发环境中,我们使用 Profiler 功能对核心代码进行了性能测试.整个加密核心算法共消耗 120309268 个时钟周期,解密核心算法需 120340755 个时钟周期,这样在选用的 167MHZ 主频的 DSP 中,加密、解密所用的时间分别为 0.7204s、0.7206s.可见系统具有良好的实时性.

6 结论

我们用 DSP 芯片实现的基于虚拟光学的信息隐藏系统,其随机模板、波长、焦距以及衍射距离的选择具有很大的自由度,这些参数组合使用构成的多维密钥,具有巨大的密钥空间,要想攻击此加密方法以获得原信息是相当困难的,系统安全性很高.同时该系统加解密速度快,可实时完成对多种多媒体数据(图像、语音、文本等)的加/解密.如用其构成嵌入式系统,可嵌入到多种电子产品中去,完成对保密图文、保密电话及各种对多媒体信息有保密要求的场合.

参考文献:

[1] P Refregier, B Javidi. Optical image encryption based on input and Fourier plane random encoding[J]. Optics Letters, 1995, 20(7): 767-769.

[2] B Javidi. Securing information by use of digital holography[J]. Optics Letters, 2000, 25(1): 28-30.

[3] O Matoba, B Javidi. Encrypted optical memory system using three-dimensional keys in the Fresnel domain[J]. Optics Letters, 1999, 24(11): 762-764.

[4] X Peng, Z Y Cui, T Tan. Information encryption with virtual-optics imaging system[J]. Optics Communications, 2002, 212(4-6): 235-245.

[5] X Peng, Z Y Cui, T Tan. Image encryption with virtual optics[A]. Proc. SPIE 4929[C]. Shanghai, China, 2002. 96-104.

[6] J W Goodman. Introduction to Fourier Optics[M]. McGraw-Hill, New York, (2nd edition), 1988.

[7] TMS320C62X/C67X CPU and Instruction Set[M]. Texas Instruments, 1998.

[8] TMS320C6X Optimizing C Compiler[M]. Texas Instruments, 1998.

作者简介:

张 鹏 男,1979 年 5 月生于河南省焦作市,博士生,主要研究信息安全、密码学理论、数字信号处理、计算机视觉等. Email: pengzhang@tju.edu.cn

彭 翔 男,1955 年 12 月生于天津市,博士、教授、博士生导师,主要研究光学信息安全、三维数字成像及造型、图像处理等. Email: xpeng@szu.edu.cn

牛憨笨 男,1940 年 2 月出生于山西壶关,教授、博士生导师,中国工程院院士,主要研究光电子学、微光夜视技术和生物医学成像技术等.