第 24 卷 第 5 期
2004 年 5 月

光 学 学 报
ACTA OPTICA SINICA

Vol. 24, No. 5
May, 2004

文章编号：0253-2239(2004)05-623-5

虚拟光学信息隐藏理论及并行硬件实现*

彭 翔[1,2] 张 鹏[2] 牛憨笨[1]

(1 深圳大学光电子学研究所 广东省光电子器件与系统重点实验室，深圳 518060
2 天津大学精密测试技术及仪器国家重点实验室，天津 300072)

摘要： 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，已成为研究的又一热点。在虚拟光学信息隐藏理论模型的基础上，使用数字信号处理器芯片的并行策略实现了一种具有多重锁、多重密钥的高密级多媒体信息隐藏系统。对系统性能的评估结果表明，该系统可以实时完成对多种数字媒体信息的加/解密，且系统性能优良。这在一定程度上弥补了虚拟光学多维数据隐藏技术所丧失的信息光学固有的并行处理能力。系统的实现为虚拟光学加密方法在现实信息加密中的应用开辟了一条有效的途径。

关键词： 信息光学；虚拟光学；加/解密；并行处理；软件流水

中图分类号：TP309.7　　文献标识码：A

Information Hiding Theory Based on Virtual Optics and Its Implementation with Parallel Hardware

Peng Xiang[1,2]　Zhang Peng[2]　Niu Hanben[1]

(1 *Key Laboratory of Optoelectronics Devices and Systems, Institute of Optoelectronics, Shenzhen University, Shenzhen* 518060
2 *National Laboratory of Precision Measurement Technology and Instrumentation, Tianjin University, Tianjin* 300072)

(Received 12 February 2003; revised 11 April 2003)

Abstract: optical encryption technology has been a subject of receiving many research efforts because of inherently parallel nature of optical information processing, high security strength and huge degree of freedom for key design. Optical security technology has appeared very promising and is likely the next generation of information security. An implementation of virtual-optics based encryption with a parallel hardware strategy is presented. A TMS320C6000 digital signal processor is used to design an information hiding system with multiple-locks and multiple-keys. An evaluation of the system performance is made and it is shown that the encryption and decryption of digital information in real-time can be achieved with such a strategy. This approach paves the way for the realization of virtual-optics based methodology by combining major advantages of optical encryption and electronic encryption.

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

1 引　　言

基于光信息处理的数据加密技术是近年来在国际上开始起步发展的一种新的“非数学”数据加密技术。与电子处理器不同，光学系统具有与生俱来的并行数据处理的能力，如在光学系统中一幅二维图

* 国家自然科学基金(60275012)资助课题、中国科学院模式识别国家重点实验室开放课题。

E-mail：xpeng@tju.edu.cn

收稿日期：2003-02-12；收到修改稿日期：2003-04-11

像中的每一个像素都可以同时地被传播和处理。当进行大量信息处理时，光学系统的并行处理能力很明显占有绝对的优势。同时，光学加密装置比电子加密装置具有更多的自由度，信息可以被隐藏在多个自由度空间中——如相位、波长、空间频率以及光的偏振态等[1~3]。我国学者在光学安全领域也做了一些有益工作[4,5]。

但是目前发展的全光学系统和光电混合数据加密系统都尚未形成可以实际应用的系统。主要原因是与电子数据加密处理器相比基于自由空间传播的光学元器件体积较大、成本很高、操作麻烦、稳定性差且处理精度低。用这样的光学元器件构造的系统难以在实际数据加密中进行应用。

本文在基于虚拟光学的信息隐藏理论模型[6,7]的基础上，使用数字处理器(DSP)芯片成功地实现了一种高密级多媒体信息加/解密系统。该系统利用电子手段(并行硬件、并行算法)模拟光学数据处理的过程，有效地将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结合起来。它利用数字仿真光学过程中传播规律和结构参量作为密钥，通过设计多重“锁”和多重“密钥”实现高安全性的数据加密。

2 基于虚拟光学的信息隐藏理论模型[6,7]

一个基于虚拟光学的信息隐藏理论增强型模型如图 1 所示。与一般模型相比其特点在于增加了用于仿真随机光场的随机模板，以提高密钥的密级。该模型克服了基于虚拟透镜成像的一般模型在实际应用时安全性不够高的缺点。

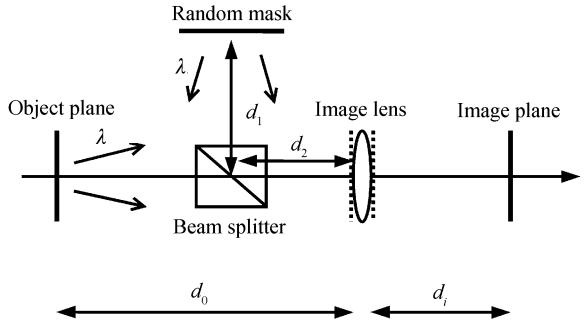

Fig. 1 Schematic diagram of enhanced model

假定信息平面和随机模板由相同选定波长的相干光照明。在加密过程中，我们用离散菲涅耳变换(DFD)计算信息平面(U_0)和随机模板(U_M)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耳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。成像透镜后表面的复振幅分布(U_{L2})被当作密文，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]：

$$U_{L2}(m,n)=\{T_{DFD}[U_0(k,l),\lambda,d_0]+T_{DFD}[U_M(k,l),\lambda,d]\}\times t(m,n,f), \quad (1)$$

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，这将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) 计算二维随机码密钥(U'_M)的离散菲涅耳变换，衍射距离为 d；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 的离散菲涅耳变换，得到原信息的像，即恢复了加密的信息。

上述解密过程可以用方程(2)描述[4]：

$$U_i(m,n)=T_{DFD}[U'(k,l),\lambda,d_i(d_0,f)], \quad (2)$$

式中

$$U'(m,n)=U_{L2}(m,n)-T_{DFD}[U'_M(k,l),\lambda,d]\times t(m,n,f), \quad (3)$$

从解密过程可以看出，要想完全解密出原信息，除了随机模板外，至少需要知道四个参量，即 d_0，f，d，λ。

3 模型的数字处理器芯片实现

我们在一块 TMS320C6701 数字处理器芯片芯片上实现了上述模型。TMS320C6701 是一种具有高并行度的高性能浮点数字信号处理器，工作频率 167 MHz，属 TI 的 C6000 系列数字处理器芯片，运行速度快，指令周期6 ns，峰值运算能力1336 Mips，硬件支持 IEEE 格式的32 bit单精度与64 bit双精度浮点操作，对于单精度浮点运算可达1 G flops[8]。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[9])在对图像做并行处理时有很好的表现。

在上述加/解密过程中，最耗时的核心循环为离散菲涅耳变换(离散菲涅耳变换)。所以我们针对离散菲涅耳变换进行了软件优化，使得加密时图像的

离散菲涅耳变换和模板的离散菲涅耳变换(二者不具有相关性)达到了并行处理。在解密时,由于两次核心离散菲涅耳变换算法具有相关性,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,使数字处理器芯片流水线始终保持充满。这些处理都在一定程度上弥补了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数字处理器芯片本身功能的限制,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。

此外,我们还使用了其它多种并行处理手段和软件优化方法,如:消除冗余循环、用双字访问两个浮点型变量、开辟数据缓冲区等。充分利用了数字处理器芯片的并行资源,在很大程度上提高了程序的性能。

4　系统性能分析

我们使用 512×512×8 bits 的灰度图[图 2(a)]进行图像信息的加/解密测试。经系统加密后的结果如图 2(b)所示。仿真随机光场的二维随机码模板是在数字处理器芯片硬件中利用德州仪器公司的 rand()函数生成的(512×512)二维伪随机阵列,如图 2(c)所示。

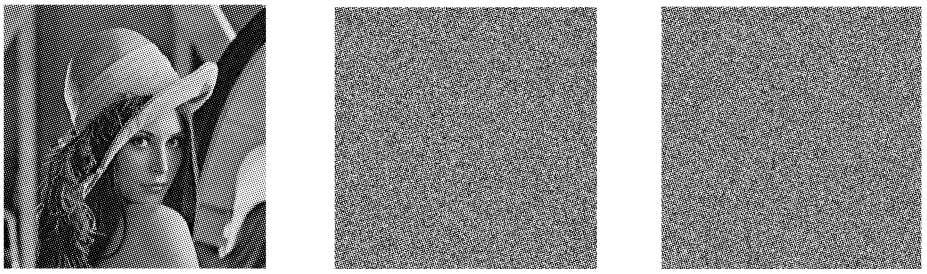

Fig. 2 (a) Original image, (b) Encrypted image, (c) Random mask

1) 密钥灵敏度

在系统测试过程中我们选择参量:波长 $\lambda=632\times10^{-9}$ m,衍射距离 $d_0=1.2$ m,透镜焦距 $f=25$ cm 作为密钥,分析各密钥的灵敏性。图 3 表示的是当 d_0 和 f 正确,但 λ 有偏差时的解密结果。

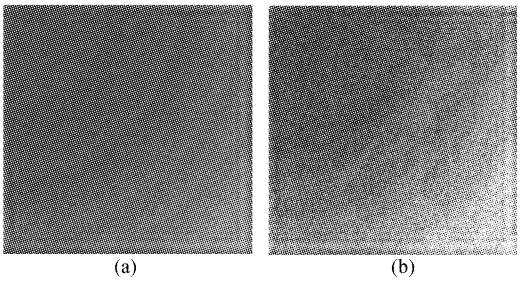

Fig. 3 Decryption results: (a) d_0 and f are correct, λ has deviations of 0.001 nm; (b) d_0 and f are correct, λ has deviation of 0.0001 nm

图 4 给出了当 λ 和 d_0 正确,但 f 有偏差时的解密结果。图 5 给出了当 f 和 λ 正确,但 d_0 存在偏差时的解密结果。

在解密时如果没有加密所用的随机模板密钥,即使参量 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 6(a)所示。只有当所有的参量正确,又知道随机模板密钥,才有可以得到清晰的解密结果,见图 6(b)。

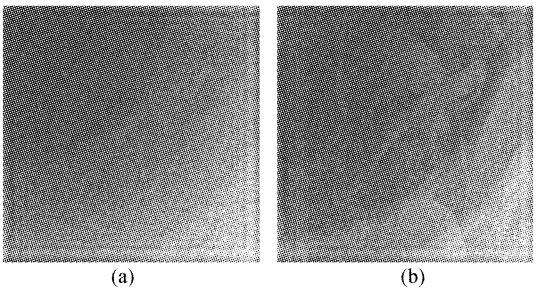

Fig. 4 Decryption results: (a) λ and d_0 are correct, f has deviations of 0.1 μm; (b) λ and d_0 are correct, f has deviations of 0.02 μm

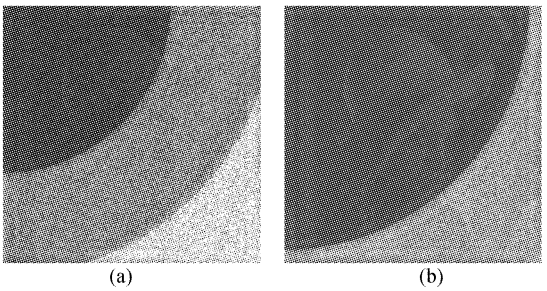

Fig. 5 Decryption results: (a) f and λ are correct, d_0 has deviations of 1 μm; (b) f and λ are correct, d_0 has deviations of 0.6 μm

(a) (b)

Fig. 6 Decryption results: (a) wrong random code, (b) all parameters are correct

从测试结果中可以看出，我们实现的加/解密系统的多重密钥中：波长的灵敏度为0.001 nm；焦距 f 的灵敏度为0.1 μm；衍射距离 d_0 的灵敏度为1 μm。

2) 图像质量的客观评价

为了定量地估计系统加/解密效果，我们引入几个客观的评价标准来评价加/解密结果的质量，它们分别是能量归一化均方误差(I_{NMSE})、等效信噪比(R_{NSNR})、图像逼真度(F_{I})，定义如下：

$$I_{\mathrm{NMSE}}=\frac{\sum_j\sum_k[f(j,k)-\hat{f}(j,k)]^2}{\sum_j\sum_k[f(j,k)]^2},\tag{4}$$

$$R_{\mathrm{NSNR}}=-10\lg(I_{\mathrm{NMSE}}),\tag{5}$$

$$F_{\mathrm{I}}=1-I_{\mathrm{NMSE}},\tag{6}$$

其中 $f(j,k)$ 为经采样后原空间图像离散图像的幅值分布、$\hat{f}(j,k)$ 为降质后离散图像的幅值分布，根据以上三式对加密后图像图 2(b)和解密后图像图 6(b)进行相应计算，结果见表 1。

Table 1 Objective evaluation of image quality

	I_{NMSE}	R_{NSNR}	F_{I}
Encrypted image	0.71962	1.429	0.28038
Decrypted image	0.024294	16.145	0.975706

从表 1 中数据可以看出，加密后图像与原图像均方误差很大，也即与原图像差异大，而它与原图像的逼真度很小，且等效信噪比很小；而解密后图像与原图像的均方误差非常小，逼真度很大，且信噪比非常高。由此可见，我们实现的高密级多媒体信息加/解密系统很好的完成了信息的加/解密工作。

3) 实时性

在德州仪器公司的 CCS (Code Composer Studio)集成开发环境中使用 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167 MHz主频的数字处理器芯片中，加密、解密所用的时间分别为 0.7204 s、0.7206 s。可见系统具有良好的实时性。

4) 为检验系统对其它多媒体信息的加/解密效果，我们对以22050 Hz采样频率进行采样的一段语音信号(以 WAV 文件格式存放于计算机硬盘上，记录声音的格式代号为 Wave_Format_PCM 格式，声音的频道数为 1，记录每个取样所需的位元数为 16 bit，除去文件头，真实的语音采样数据为512 kB)进行语音信息加/解密测试。用于加密的语音波形如图 7(a)所示，语音经系统加密后波形如图 7(b)所示，由解密端解密后的语音波形如图 7(c)所示。

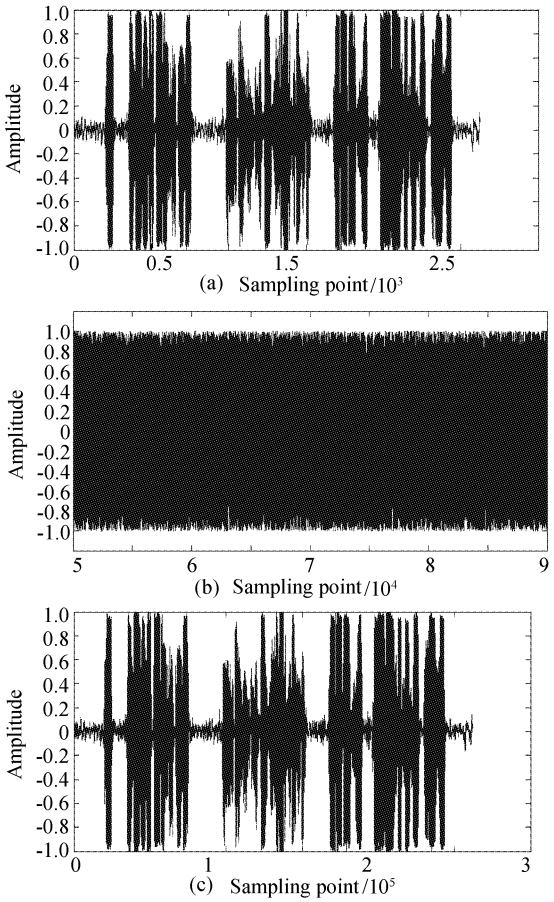

Fig. 7 Audio signal security: (a) original signal; (b) encrypted signal; (c) decrypted signal

测试结果证明，用数字处理器芯片实现的基于虚拟光学的信息隐藏系统同样成功地完成了对语音信息的隐藏和提取。

结论 本文在虚拟光学信息隐藏理论模型的基础上，给出了用数字处理器芯片芯片实现该理论模型的具体方法，同时还对虚拟光学信息加/解密系统的性能进行了实验分析。结果验证了基于虚拟光学的信息隐藏理论的有效性，以及利用数字处理器芯片并行处

理策略实现虚拟光学加密/解密的可行性。将光学数据加密的思想与电子数据加密处理器相结合，可以同时兼顾光学处理和电子处理的各自优点，为虚拟光学的信息隐藏理论的实际应用奠定了基础。

参 考 文 献

1 Refregier P, Javidi B. Optical image encryption based on input and Fourier plane random encoding. *Opt. Lett.*, 1995, **20**(7): 767～769

2 Javidi B. Securing information by use of digital holography. *Opt. Lett.*, 2000, **25**(1): 28～30

3 Matoba O, Javidi B. Encrypted optical memory system using three-dimensional keys in the Fresnel domain. *Opt. Lett.*, 1999, **24**(11): 762～764

4 Huang Qizhong, Du Jinglei, Zhang Yixiao *et al*.. Implementation of information decomposing using CGH and its applications in optical image encryption. *Chin. J. Lasers* (中国激光), 2000, **27**(10): 903～906 (in Chinese)

5 Cao Hanqiang, Zhu Guangxi, Zhu Yaoting *et al*.. A method based on hypercomplex number system for fractal digital hologram synthesis. *Acta Optica Sinica* (光学学报), 2001, **21**(1): 114～117 (in Chinese)

6 Peng X, Cui Z Y, Tan T. Information encryption with virtual-optics imaging system. *Opt. Commun.*, 2002, **212**(4～6): 235～245

7 Peng X, Cui Z Y, Tan T. Image encryption with virtual optics. *Proc. SPIE*, 2002, **4929**: 96～104

8 TMS320C62X/C67X CPU and Instruction Set. Texas Instruments, 1998. http://www.ti.com

9 TMS320C6X Optimizing C Compiler, Texas Instruments, 1998. http://www.ti.com