第 59 卷 第 3 期 2010 年 3 月
1000-3290/2010/59(03)/1762-07

物 理 学 报
ACTA PHYSICA SINICA

Vol. 59, No. 3, March, 2010

基于非线性级联傅里叶变换的光学 Hash 函数构造*

何文奇[1)†] 彭 翔[1)‡] 祁永坤[1)] 孟祥锋[1)] 秦 琬[1)] 高 志[2)]

1)(深圳大学光电工程学院,光电子器件与系统教育部/广东省重点实验室,深圳 518060)

2)(Clemson 大学生物医学工程系, 501-5 Rhodes Research Center, Clemson, SC 29634, USA)

(2009 年 5 月 7 日收到;2009 年 6 月 9 日收到修改稿)

提出一种基于非线性级联傅里叶变换的光学 Hash 函数的构造方法. 此方法分为两轮单向加密过程,在第一轮中,先将待处理的数字信息以 512 bit 作为数据块编码,将整个数字信息整分成若干个"8×8 的 256 阶灰度图像"(信息平面),然后在光电混合系统中对上述信息平面组做非线性级联傅里叶变换得到一个数值矩阵,对其进行扩展后得到 4 个信息平面,再对它们做非线性级联傅里叶变换得到 64 bit 的 Hash 值($hash_1$);在第二轮中,先将原始信息平面中的每个数值循环左移 4 位,构造出相应的辅助信息平面组,然后对其做与第一轮相同的单向加密操作,得到 $hash_2$,将其与之前生成的 $hash_1$ 组合起来构成最终 128 bit 的 Hash 值(hash). 同时,本文提出采用雪崩效应系数(AEC)作为评价光学 Hash 函数性能的参数,理论分析和仿真实验均表明,该方法构造的光学 Hash 函数具有很好的抗碰撞性和良好的雪崩效应.

关键词: 信息光学, 光学 Hash 函数, 非线性级联傅里叶变换, 雪崩效应

PACC: 4230K, 4230D

1. 引 言

在当今数字网络迅速普及的背景下,特别是随着电子商务、电子政务的快速发展,消息认证、身份认证和数字签名等技术已成为人们日益关注的焦点[1—4],而 Hash 函数的构造正是实现各种认证方案的关键技术. Hash 函数是一种单向密码体制,只有加密过程,不能解密[5]. 自 1990 年 Rivest 构造出 MD4[6] 以来,国际密码学界先后构造了 MD5, SHA-0, SHA-1, PIPEMD-160, SHA-256, SHA-384, SHA-512 等 Hash 函数[5,7],安全性能不断提高. 其中,MD5 和 SHA-1 是当前应用最为广泛的两种 Hash 函数,很多文件在互联网上开放下载的同时都提供一个 MD5 的信息摘要,使下载方能够确认所下载的文件与原文件一致,以此来防止文件被篡改. 然而,MD5 和 SHA-1 最近已经先后被发现可能存在安全隐患[8,9]. 上述各类 Hash 算法都是基于各种数学难题和数学运算构造的. 近年来,量子密码学、光学密码学、神经网络密码学等基于非数学构造的密码学逐渐兴起. 相比于传统的密码算法,这些新型密码算法都有其自身固有的优点[10—12]. 已有学者开始构造基于物理过程的 Hash 函数,如基于混沌神经网络的 Hash 函数[13],基于混沌映射的 Hash 函数[14], 而由于各种光学变换的线性性质,导致基于光学思想的各种密码体制几乎都属于对称密码体系[12, 17, 18],尽管最近一些方案尝试了非对称密码体制[15, 16],但这些方案都无法满足当今数字网络安全的需求,譬如数据完整性认证,身份认证等,因此如何构造出基于光学思想的 Hash 函数成为了光学信息安全领域发展过程中所面临的一个重大问题.

本文在"虚拟光学"[17, 18] 的框架下,提出一种基于"非线性级联傅里叶变换"的光学 Hash 函数的构造方法,利用多次光学傅里叶变换和多次替换相

* 国家自然科学基金(批准号:60907005,60775021),中科院微系统与信息技术研究所项目和中国博士后科学基金(批准号:200902334)资助的课题.

† E-mail: winckay@hotmail.com

‡ E-mail: xpeng@szu.edu.cn

位的非线性操作，实现对信息的单向加密和数据压缩功能，生成 128 bit 的 Hash 值. 本文利用计算机进行了大量的仿真实验和相关的攻击测试，结果表明，此方案能够满足 Hash 函数所要求的单向性、压缩性、抗碰撞性和初值敏感性等要求.

2. Hash 函数[5]

Hash 函数是满足以下要求的一类函数.

2.1. 基本要求

1）算法公开，不需要密钥.

2）有数据压缩功能，能将任意长度的输入转换成一个固定长度的输出.

3）容易计算. 即给出任意信息 m，要计算出 Hash 值 $h(m)$ 是容易的.

2.2. 安全性要求

1）给定信息的 Hash 值 $h(m)$ 要求出 m 是计算上不可行的. 即对给定的一个 Hash 值，不可能找出一条信息使其 Hash 值正好是给定的，这就是单向性.

2）给定信息 m 和其 Hash 值 $h(m)$，要找到另一个与 m 不同的信息 m'，使得它们的 Hash 值相同是不可能的（即抗弱碰撞性）.

3）对于任意两个不同的信息 m 和 m'，它们的 Hash 值不可能相同（即抗强碰撞性），实际上任意两个信息如果略有差别，它们的 Hash 值也会有很大的不同，即雪崩效应.

3. 非线性级联傅里叶变换

基于光学傅里叶变换的加密算法都具有线性和可逆性质，而 Hash 函数是单向的不可逆加密，这使得基于光学傅里叶变换的加密系统在构建 Hash 函数时遇到很大困难. 本文的基本思想是，由数值矩阵构造出复振幅并对其连续多次作傅里叶变换，每次傅里叶变换后去除或替换其相位，可构造出理论上不可逆的光学装置，这一过程既利用了傅里叶变换对信息的混淆和扩散作用，又实现了对输入数据的压缩机理，使得用光学方法构造 Hash 函数成为可能. 图 1 是理论上可实现上述功能的非线性级联傅里叶变换的光电混合系统模型，其中 SLM_1（Spatial Light Modulator），SLM_2 代表两个空间光调制器，它们在上述系统中分别用来动态调制振幅和相位；LENS，PC 和 CCD 分别代表透镜、计算机和电荷耦合器件（量化精度为 12 位）；f，Electronic Control 分别代表透镜焦距和数字空间的电子操作.

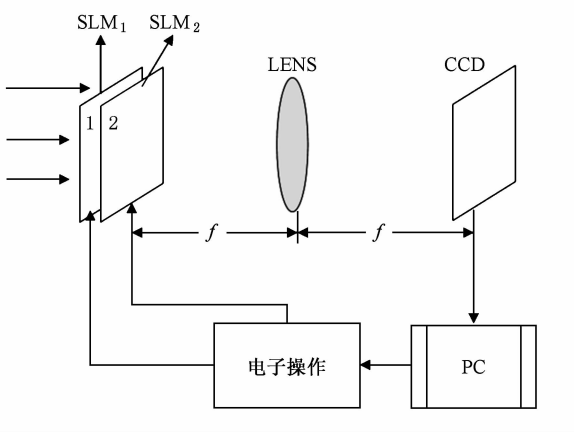

图 1　非线性级联傅里叶变换光电混合系统模型

此非线性级联傅里叶变换光电混合系统的工作方式：假设有 N 个数值矩阵（灰度图像，M_1，M_2，…，M_N），首先利用 PC 将数值矩阵 M_1 调制成振幅写入 SLM_1，将数值矩阵 M_2 调制成相位写入 SLM_2，从而构成第一个复振幅 t_1. 然后，用平行光照射，通过透镜傅里叶变换后，用焦距处的高精度 CCD 记录其频谱图，再将 PC 处理后的频谱图写入 SLM_1，同时再将数值矩阵 M_3 调制成相位写入 SLM_2，构成第二个复振幅 t_2，再通过透镜逆傅里叶变换后，用 CCD 记录其频谱图，PC 处理此频谱图后，再将其写入 SLM_1……如此循环操作，直到将数值矩阵 M_N 调制成相位写入 SLM_2，构成第（N-1）个复振幅 $t_{(N-1)}$，通过透镜傅里叶变换后，最终在 CCD 上获得一个频谱图，此过程便是“非线性级联傅里叶变换”的实现过程.

4. 光学 Hash 函数的构造方法

本文提出的光学 Hash 函数的构造方法分为两轮单向加密，并由这两轮单向加密生成的 Hash 值组合成最终 128 bit 的 Hash 值.

4.1. 第一轮单向加密过程

首先将待处理的数字信息以 512 bit 进行分块编码，最后不足 512 bit 的数据块填充 1（每次至少处理 $2\times512=1$kbit 数据）. 如图 2，以处理 $512\times N$bit 数据为例，分成 N 个 8×8 的数值矩阵（M_1，M_2，…，M_N），

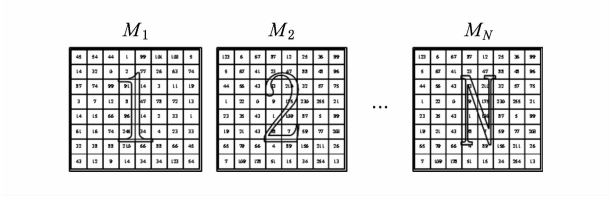

图 2 信息平面

其中每个数值均为 0—255 之间的整数,我们把这些数值矩阵称为“信息平面”,也可看成是一组 8×8 的 256 阶灰度图像.

接下来将上述 N 个信息平面置于图 1 所示光电混合系统,对其做“非线性级联傅里叶变换”得到另一个 8×8 的数值矩阵 M',其中每个数值均为 0—255 之间. 其算法流程如图 3 所示,具体步骤如下:

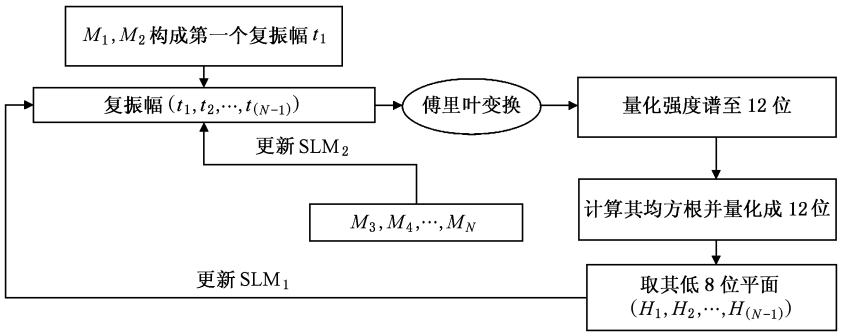

图 3 非线性级联傅里叶变换算法流程图

1)将 M_1(数值矩阵 1)调制为振幅写入 SLM_1,将 M_2 归一化后调制为相位写入 SLM_2,构造出输入域的初始复振幅 t_1,具体表达式可写为

$$t_1 = M_1 \cdot \exp(j2\pi M_2/255). \quad (1)$$

2)用平行光照射 t_1,经过光学傅里叶变换后,用 CCD 在透镜后焦平面记录强度谱(量化成 12 位),通过 PC 操作,对其开方运算后将结果量化成 12 位,并取其低 8 位得到 H_1,具体表达式可写为

$$H_1 = Q_{12\to 8}\{\mathrm{SQRT}[Q_{12}(\mathrm{FT}(t_1))]\}, \quad (2)$$

式中 FT(.)表示傅里叶变换,$Q_{12}(.)$表示记录并量化强度谱到 12 位,SQRT(.)表示开方运算,$Q_{12\to 8}(.)$表示量化到 12 位并取其低 8 位. 此过程是一个非线性傅里叶变换运算,即本文光学 Hash 函数构造算法中的基本处理单元,也称为压缩函数,此函数有两个输入和一个输出. 引入算子 NFT[.]描述压缩函数,上述步骤 1,2 可写为

$$\begin{aligned} H_1 &= \mathrm{NFT}[M_1, M_2] \\ &= Q_{12\to 8}\{\mathrm{SQRT}[Q_{12}(\mathrm{FT}\{M_1 \\ &\quad \times \exp(j2\pi M_2/255)\})]\}. \end{aligned} \quad (3)$$

3)将 H_1 调制成振幅更新 SLM_1,同时将 M_3 归一化后调制成相位更新 SLM_2,构造出第二个复振幅 t_2,然后用平行光照射 t_2,经过光学傅里叶变换后,用 CCD 在透镜后焦平面记录强度谱(量化成 12 位),通过 PC 操作,对其开方运算后将结果量化成 12 位,并取其低 8 位得到 H_2. 利用算子 NFT[.]描述此步骤,其表达式可写为

$$\begin{aligned} H_2 &= \mathrm{NFT}[H_1, M_3] \\ &= Q_{12\to 8}\{\mathrm{SQRT}[Q_{12}(\mathrm{FT}\{H_1 \\ &\quad \times \exp(j2\pi M_3/255)\})]\}. \end{aligned} \quad (4)$$

4)重复使用此压缩函数($N-1$)次,可将 N 个信息平面全部关联起来,以完成非线性级联傅里叶变换过程. 其中第 k ($1<k<N$)次使用压缩函数的具体表达式可写为

$$\begin{aligned} H_{(k)} &= \mathrm{NFT}[H_{(k-1)}, M_{(k+1)}] \quad (1<k<N) \\ &= Q_{12\to 8}\{\mathrm{SQRT}[Q_{12}(\mathrm{FT}\{H_{(k-1)} \\ &\quad \times \exp(j2\pi M_{(k+1)}/255)\})]\}. \end{aligned} \quad (5)$$

为方便下文的叙述,引入算子 NCFT[$M_1, M_2,$

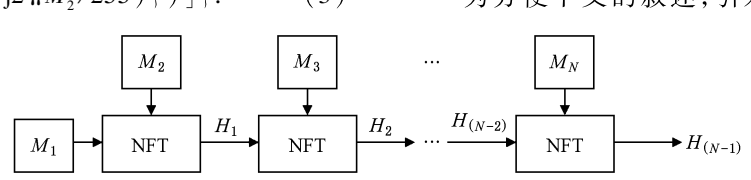

图 4 非线性级联傅里叶变换的结构图

…,M_N]来描述整个非线性级联傅里叶变换过程,如图 4,具体表达式可写为

当 $N=2$ 时,

$$\begin{aligned} M' &= H_{(N-1)} = H_1 \\ &= \mathrm{NCFT}[M_1, M_2, \cdots, M_N] \\ &= \mathrm{NFT}[M_1, M_2]; \end{aligned} \tag{6}$$

当 $N>2$ 时,

$$\begin{aligned} H_1 &= \mathrm{NFT}[M_1, M_2], \\ M' &= H_{(N-1)} \\ &= \mathrm{NCFT}[M_1, M_2, \cdots, M_N] \\ &= \mathrm{NFT}[\cdots \mathrm{NFT}[\mathrm{NFT}[H_1, M_3], M_4], \cdots, \\ &\quad M_{(N-1)}], M_{(N)}]. \end{aligned} \tag{7}$$

为进一步增强此光学 Hash 函数的扩散和混淆作用,同时增强输出结果与原始信息每个 bit 位的关联性,再将 M'划分成 4 个 4×4 的数值矩阵(M_a, M_b,M_c,M_d),通过 PC 对其进行数值操作,对 M_a—M_d 中的每个数值进行扩展,复制为 4 个相同的值(如图 5 所示),得到 4 个 8×8 的数值矩阵(M_A, M_B,M_C,M_D),再对其做非线性级联傅里叶变换处理,得到一个 8×8 的数值矩阵 M'', 其中每个数值均为 0—255 之间. 利用 NCFT 算子,表达式如下:

$$M'' = \mathrm{NCFT}[M_A, M_B, M_C, M_D]. \tag{8}$$

至此完成了第一轮单向加密过程. 此时,按照一定规则在 M''中任意选取 8 个数值. 本文选取的是左上角至右下角对角线上 8 个 8 位数值,构成 hash_1(64 bit).

值得注意的是,在上述非线性级联傅里叶变换过程中,对每次写入 SLM_1 的数值矩阵,都必须先利用 PC 对其做“去零化”处理,否则有零的位置将对更新在其上的相位板上相应数值的变化不敏感,从而暗藏了碰撞的机会,其具体处理方式可表示为

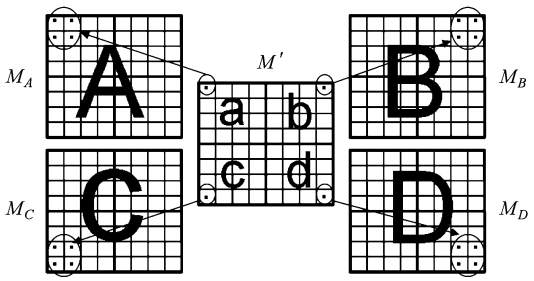

图 5　扩展数值矩阵

$$\begin{aligned} M(i,j)' &= M(i,j) + k \\ &(M_k(i,j) \leqslant (255 - k)), \\ M(i,j)' &= M(i,j) + k - 255 \\ &(M_k(i,j) > (255 - k)), \end{aligned} \tag{9}$$

其中 $M(i,j)$表示处理前的数值矩阵, $M(i,j)'$表示“去零化”处理后的数值矩阵,k 的取值范围是 0—255,本文仿真实验所采用的 k 值为 3.

4.2. 第二轮单向加密过程

下面进行第二轮单向加密,其过程和原理与第一轮操作一样,只是在处理信息平面之前,先对各个信息平面中的每个数值做一个循环移位的操作,从而构造出对应的辅助信息平面. 具体实现方法如下:每个信息平面含有 8×8 个 8 位的数值,对每个数值进行位操作,使其循环左移 4 位,例如:信息平面中一个数值为 150,其二进制表示为 10010110,循

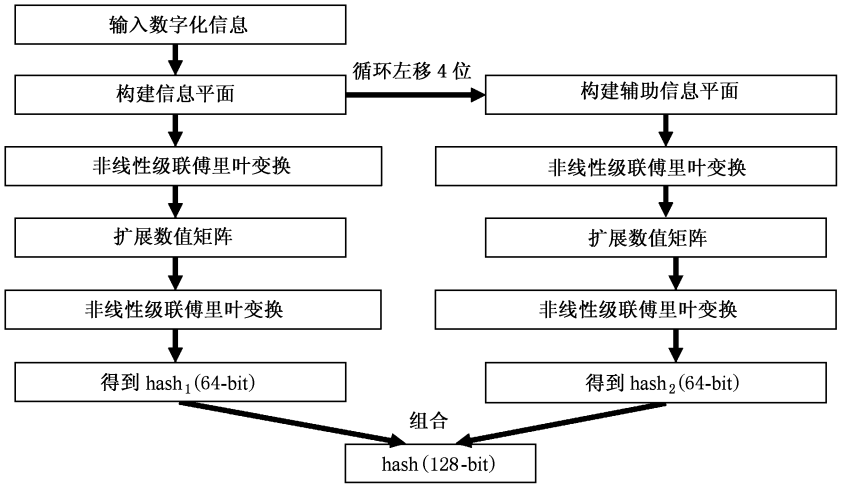

图 6　光学 Hash 函数流程图

环左移 4 位后得到 01101001,即 105.

接下来对构造出的 N 个辅助信息平面做非线性级联傅里叶变换,其具体过程如上述第一轮单向加密过程,最后同样得到 64 bit 的 $hash_2$. 结合第一轮单向加密所得的 64 bit 的 $hash_1$,最终得到光学 Hash 值,共 128 bit.

第二轮单向加密中的移位操作,其目的在于扩大某些对信息平面的轻微篡改,使得 Hash 值能够以更大的变化幅度对信息平面的轻微篡改做出响应,从而使得 Hash 值具有更好的普适性和雪崩效应.

整个光学 Hash 过程如图 6 所示.

5. 仿真实验及测试结果

本文在 MATLAB R2008a 环境下,仿真实现了基于非线性级联傅里叶变换的光学 Hash 构造.

5.1. 雪崩效应检测

针对光学 Hash 函数的特点,本文提出以雪崩效应系数(AEC)作为评价 Hash 函数性能的测度,定义如下:

$$AEC = \mathrm{diff}(H,H')/128, \qquad (10)$$

式中 H,H' 分别表示对原始信息和篡改后的信息做光学 Hash 运算所得的 Hash 值,diff[.]表示计算两个 Hash 值中 bit 位不同的个数. 其含义为:对一组随机信息来说,对其做篡改,其 AEC 值越大,则说明雪崩效应越好;而如果 AEC 值为 0,则说明出现碰撞现象. 通常 MD5,SHA-1 等 Hash 函数,其雪崩效应系数都大致等于 0.5.

随机产生 10,100,1000 kbit 的数字信息各一组,并将其按上文要求分别初始化成若干个信息平面,分别做 10000 次攻击,每次随机改变其中的一个 bit 位,分别计算出其 AEC 值并求平均.

表 1 雪崩效应测试结果

数据大小/kbit	AEC			单次 Hash 运算时间/s
	最小值	最大值	平均值	
10	0.28	0.67	0.49	0.0207
100	0.31	0.66	0.49	0.0716
1000	0.35	0.67	0.49	1.7803

由表 1 可知:此光学 Hash 函数针对不同尺寸的数字信息均具有较好的雪崩效应,对原始数字信息的变动有较强的敏感性,能够很好的满足 Hash 函数的性能要求.

值得说明的是:如果在构造此光学 Hash 函数时,省去图 5 所示的数值扩展并再次做非线性级联傅里叶变换等操作,然后对其做相同的攻击测试,则 AEC 的最小值分别为 0.17,0.18 和 0.20,不具有明显的雪崩效应.

5.2. 抗碰撞性检测

实验中,我们通过以下方法定量测试 Hash 函数的抗碰撞能力[19]:随机地选取一定量的数字信息,求出 Hash 值并以 ASCII 码形式存储(共 16 个 ASCII 码字符),然后随机地选择并改变数字信息中 1 个 bit 位得到另一新的 Hash 值,同样以 ASCII 码形式存储其 Hash 值. 比较两个 Hash 结果,若两个 Hash 值中有一个相同位置上 ASCII 码字符相同,则称为被击中一次,统计被击中的次数以及每次被击中的 ASCII 码字符的个数,若被击中一个字符,则称为 One-shot;若被击中两个字符,则称为 Two-shot.

做 1000 次试验,每次分别随机产生 10,100,1000 kbit 的数字信息,按照上述方法,分别统计被击中的次数以及每次被击中的 ASCII 码字符的个数.

表 2 抗碰撞性检测结果

数据大小/kbit	10	100	1000
One-shot 次数	117	112	118
Two-shot 次数	3	3	3

由于 Hash 值是 16 个 ASCII 码字符,由表 2 可知:在 1000 次试验中,出现 1/16 相同字符的概率分别是 11.7%,11.2% 和 11.8%,而出现 1/8 相同字符的概率分别为 0.3%,0.3% 和 0.3%. 此光学 Hash 函数对不同尺寸的数据均显示出很好且稳定的抗碰撞性能.

6. 结 论

提出一种基于非线性级联傅里叶变换的光学 Hash 函数的构造方法,首次构造出了基于光学概念的 Hash 函数. 该方法利用空间光调制器、高精度 CCD、光学透镜和计算机组成的混合光电系统,进行两轮单向加密和压缩过程,最终得到 128 bit 的 Hash 值,且此光学 Hash 函数具有光信息处理固有的高速并行性,大容量等固有的优势,同时理论分析和仿真测试实验都证明其结果很好的满足了 Hash 函数所要求的抗碰撞性和雪崩效应等性能要求.

[1] Tsudik G 1992 *Comput. Commun. Rev.* **22** 29

[2] Yang Y G 2008 *Chin. Phys.* B **17** 415

[3] Schneier B 1996 *Applied Cryptography*, *second edition* (John Wiley & Sons) p122—177

[4] Shimon E, Goldreich O, Micali S 1996 *J. Cryptology* **9** 35

[5] Hu X D, Wei Q F 2005 *Applied Cryptography tutorial* (Beijing: Electronics industry Press) p122—177 (in Chinese) [胡向东、魏琴芳 应用密码学教程 2005 (北京:电子工业出版社) 第 122 页—177 页]

[6] Rivest R L 1991 *Lect. Notes. Comput. Sc.* **537** 303

[7] Rivest R L 1992 *RFC* 1321, *MIT and RSA Data Security*, *Inc*

[8] Wang X Y, Yu H B 2005 *Lect. Notes. Comput. Sc.* **3494** 19

[9] Wang X Y, Yin Y L, Yu H B 2005 *Lect. Notes. Comput. Sc.* **3621** 17

[10] Lin Q Q, Wang F Q, Mi J L, Liang R S, Liu S H 2007 *Acta. Phys. Sin.* **56** 5796 (in Chinese) [林青群、王发强、米景隆、梁瑞生、刘颂豪 2007 物理学报 **56** 5796]

[11] Cai J M, Liu D, Chen T M 2007 *Comput. Appl.* **27** 219 (in Chinese) [蔡家楣、刘　多、陈铁明 2007 计算机应用 **27** 219]

[12] Refregier P, Javidi B 1995 *Opt. Lett.* **20** 767

[13] Liu G J, Shan L, Dai Y W, Sun J S, Wang Z Q 2006 *Acta. Phys. Sin.* **55** 5688 (in Chinese) [刘光杰、单　梁、戴跃伟、孙金生、王执铨 2006 物理学报 **55** 5688]

[14] Wang J Z, Wang Y L, Wang M Q 2006 *Acta. Phys. Sin.* **55** 5048 (in Chinese) [王继志、王应龙、王美琴 2006 物理学报 **55** 5048]

[15] Peng X, Wei H Z, Zhang P 2006 *Opt. Lett.* **31** 3579

[16] Yuan S, Zhou X, Alam M S, Lu X, Li X F 2009 *Opt. Express* **17** 3270

[17] Peng X, Yu L F, Cai L L 2002 *Opt. Express* **10** 41

[18] Peng X, Tang H Q, Tian J D 2007 *Acta. Phys. Sin.* **56** 2629 (in Chinese) [彭　翔、汤红乔、田劲东 2007 物理学报 **56** 2629]

[19] Yi X 2005 *IEEE T. Circuits. Syst.* **52** 354

Construction of optical Hash function based on nonlinear cascaded Fourier transform*

He Wen-Qi[1)†] Peng Xiang[1)‡] Qi Yong-Kun[1)] Meng Xiang-Feng[1)] Qin Wan[1)] Bruce Z. Gao[2)]

1)(*College of Optoelectronics Engineering, Key Laboratory of Optoelectronic Devices and Systems of Ministry of Education and Guangdong Province, Shenzhen University, Shenzhen* 518060, *China*)

2)(*Department Biomedical Engineering, Clemson University*, 501-5 *Rhodes Research Center, Clemson, SC* 29634 *USA*)

(Received 7 May 2009; revised manuscript received 9 June 2009)

Abstract

A method of constructing optical Hash function based on nonlinear cascaded Fourier transform is proposed. The proposed method consists of two single one-way encryption processes. In the first process, the digital information is divided to several data blocks with 512-bit each. The data blocks are encoded to 8 by 8 sub-images with 256 gray scales, creating information planes. Then take a nonlinear cascaded Fourier transform of sub-image to generate a data matrix through an optical/digital hybrid system. By extending the data matrix we get four information planes. Again, taking nonlinear cascaded Fourier transform to built information planes, we get a Hash value 64-bit long ($hash_1$). In the second process, we shift cydically every numerical value of the original information planes by 4-bit, constructing auxiliary information planes. Thereafter we take the same operations as we have done in the first process to the Hash value ($hash_2$). Once $hash_1$ and $hash_2$ obtained, they are combined to form a final Hash value 128-bit long (hash). Furthermore, the avalanche effect coefficient (AEC) was also proposed to evaluate the performance of the optical Hash function. Theoretical analysis and simulation results are presented to show the effectiveness of optical Hash function constructed by our approach and the constructed optical Hash function has good performance of avalanche effect and collision resistance.

Keywords: information optics, optical Hash function, nonlinear cascaded Fourier transform, avalanche effect

PACC: 4230K, 4230D

* Project supported by the National Natural Science Foundation of China (Grant Nos. 60907005, 60775021), the Shanghai Institute of Microsystems and Information Technology and the China Postdoctoral Science Foundation Project (Grant No. 200902334).

† E-mail: winckay@hotmail.com

‡ E-mail: xpeng@szu.edu.cn