物理学报 Acta Physica Sinica
Chinese Physical Society
Institute of Physics, CAS

一种基于多重散射的光学Hash函数

何文奇　陈嘉誉　张莲彬　卢大江　廖美华　彭翔

Optical Hash function based on multiple scattering media

He Wen-Qi　Chen Jia-Yu　Zhang Lian-Bin　Lu Da-Jiang　Liao Mei-Hua　Peng Xiang

引用信息 Citation: Acta Physica Sinica, 70, 054203 (2021)　DOI: 10.7498/aps.70.20201492
在线阅读 View online: https://doi.org/10.7498/aps.70.20201492
当期内容 View table of contents: http://wulixb.iphy.ac.cn

一种基于多重散射的光学 Hash 函数*

何文奇 陈嘉誉 张莲彬 卢大江 廖美华† 彭翔‡

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

(2020 年 9 月 7 日收到; 2020 年 11 月 5 日收到修改稿)

本文提出了一种基于光与多重散射介质相互作用的光学 Hash 函数构造方法. 该方法创新性地利用多重散射介质对相干调制光的天然随机散射作用, 实现了对调制光的“混淆”和“扩散”, 从而满足了 Hash 函数的核心功能要求: 高安全强度的单向编码/加密. 所设计的光电混合系统能有效地模拟 Hash 函数中的“压缩函数”, 结合具有特征提取功能的 Sobel 滤波器, 能实现将任意长度的输入数据压缩并加密为固定长度为 256 bit 的输出 (即 Hash 值). 一系列仿真结果表明: 该方法所构造的光学 Hash 函数具有良好的“雪崩效应”和“抗碰撞性”, 其安全性能可比拟当前最为广泛使用的传统 Hash 函数 (MD5 和 SHA-1).

关键词: 光学信息安全, 光学 Hash 函数, 多重散射介质, 雪崩效应

PACS: 42.30.Kq, 42.25.Dd, 42.25.Fx **DOI:** 10.7498/aps.70.20201492

1 引 言

随着信息技术和互联网的发展, 人类进入了“信息爆炸”的时代. 信息的爆炸式增长促进了人类社会的发展, 但是, 伴随而来的信息安全问题也引起了人们的广泛关注, 如何保证信息的安全性也成为了一个持续的研究热点. 目前, 信息安全技术通常可分为两大类, 一类是基于数学运算的传统信息安全技术; 另一类是基于非数学运算的新型信息安全技术, 主要包括: 量子加密、生物特征识别和光学信息安全[1] 等. 其中, 得益于“光学信息处理”具有并行处理以及多维运算的能力, 光学加密技术近年来吸引了不少学者们的关注. 自 Refregier 和 Javidi[2] 于 1995 年提出基于 $4f$ 光学相关器的双随机相位编码技术以来, 研究者们在此基础上发展出了一系列相关的衍生技术[3−5]. 但是, 由于双随机相位编码系统具有线性以及对称性, 导致其存在一定的安全隐患, 这一点已经被多种密码分析方案所证实[6−8]. 为了解决这一问题, 各国的研究者们陆续在此基础上提出了多种安全性增强型的光学加密方案[9,10], 甚至是加、解密钥不同的光学非对称密码系统[11−16].

众所周知, 在信息安全领域中, 除了“加密”技术之外, 各类安全认证技术也同等重要, 其中, Hash 函数便是一种能够高效地实现“数据完整性认证”的核心技术, 同时, Hash 函数也在数字签名、数据检索以及身份认证等众多领域扮演着非常重要的角色[1]. 通常, 我们将 Hash 函数视为一个单向加密系统, 它能将任意长度的输入消息 M 映射为固定长度的输出 h, 即 $h = H(M)$. 为了保证其安全性, Hash 函数需满足以下三个条件: 1) 对于给定的 M, 易于计算出其对应的 Hash 值 h; 2) 对于给定的 h, 难以计算出 M; 3) 对于给定的 M, 难以找到另一个消息 M', 使得 $H(M)= H(M')$, 即抗碰撞性[1]. 在传统信息安全领域, 自 MD4[17] 算法

* 国家自然科学基金 (批准号: 61875129, 61705141, 61805152)、中德合作项目 (批准号: GZ1391, M-0044) 和广东省自然科学基金 (批准号: 2018A030310561) 资助的课题.

† 通信作者. E-mail: liaomeihua@outlook.com

‡ 通信作者. E-mail: xpeng@szu.edu.cn

在 1990 年被提出以来, Hash 函数已取得了长足的进步. 目前, 应用最广泛的 Hash 函数有两大系列, 即 MD 系列 [17] 以及 SHA 系列 [18], 其中, MD5 和 SHA1 是国际上通行的两大 Hash 函数. 值得指出的是: 这两种主流 Hash 函数都是基于某种数学难题和复杂的数学运算而设计的. 近年来, 在光学信息安全领域, 几种基于光学思想和理论的 Hash 函数也相继被提出, 如 2010 年, He 等 [19,20] 首次提出了一种基于级联切相傅里叶变换的光学 Hash 函数, 从理论上探索了用光电混合系统构建 Hash 函数的可能性. 随后, Lai 等 [21] 又提出了一种基于双光束干涉的光学 Hash 函数, 并对其安全性能进行了系统分析. 然而, 上述两种方法的核心部件——压缩函数, 其本质上都是一个线性过程, 尽管均引入了非线性操作, 但其理论上的安全隐患仍然存在.

本文将提出一种基于光与多重散射介质相互作用的光学 Hash 函数. 在该方法中, 以多重散射介质来构造核心部件——光学压缩函数, 创新性地利用多重散射介质与相干调制光的相互作用, 进行天然而充分地随机“扰乱”, 实现对调制光的“混淆”和“扩散”. 文中将详细描述所提光学 Hash 函数的设计过程, 并给出相应的数值仿真实验和结果分析.

2 Hash 函数的一般结构

Hash 函数的一般结构如图 1 所示, 它是一种基于消息预编码的迭代结构, 通过级联调用一个压缩函数, 每次处理一个固定长度的消息分组, 最终输出一个固定长度的 Hash 值. 可以看出, 其核心是压缩函数 f, 它以某一个消息分组 M_i (i = 1, 2, 3, ···, t) 和上一个压缩函数的输出 H_i (i = 2, 3, ···, t) 为输入, 输出为 H_{t+1}. Hash 函数算法还需要一个初始值 H_1 以及变换函数 g, 其中, 变换函数 g 的作用是将压缩函数的最终输出 H_{t+1} 转化成固定长度的 Hash 值. 用数学形式可将整个 Hash 算法表示为:

$$H_{i+1} = f\left(M_i, H_i\right)(i = 1, 2, \ldots, t), \tag{1}$$

$$h\left(M\right) = g\left(H_{t+1}\right). \tag{2}$$

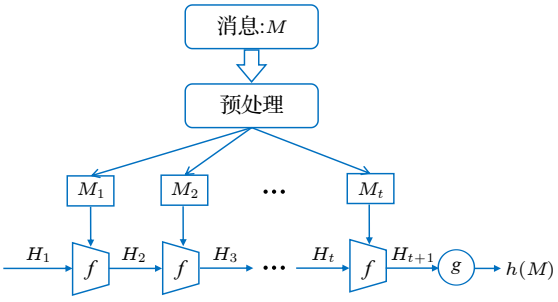

图 1 Hash 函数的结构

Fig. 1. Schematic diagram of the Hash function.

3 基于多重散射的光学压缩函数

如上所述, 压缩函数是 Hash 函数的核心单元, 因此, 它的实现方式在很大程度上决定了 Hash 函数的性能优劣. 本文利用多重散射介质对相干调制光的天然而变幻莫测的“扰动效应”, 选择以“多重散射介质”作为压缩函数的核心部件来构造光学 Hash 函数. 拟用于实现基于多重散射的光学压缩函数的光电系统结构如图 2 所示, 其中, SF 表示空间滤波器; L 表示准直透镜; SLM_1 和 SLM_2 分别表示振幅型空间光调制器和纯相位型空间光调制器, 用于加载待处理的消息分组 (复振幅分布); MSM(multiple scattering medium) 表示多重散射介质; D 表示孔径光阑. 受 SLM 调制的光经过多重散射介质时将以不可预知的方向随机散射, 因此, 携带调制消息的光波将由于光的多重散射效应而被多次“混淆”和“扩散”.

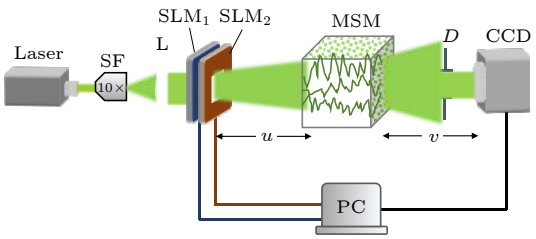

图 2 实现基于多重散射的光学压缩函数的光电系统结构示意图

Fig. 2. Schematic diagram of optoelectronic architecture for realizing the optical compression function based on multiple scattering.

该光学压缩函数的具体工作原理和流程如下: 1) M_i (i = 1, 2, 3, ···, t) 以及 H_i (i = 1, 2, 3, ···, t) 被编码为 8 位量化精度、大小为 16 × 16 像素的图像, 并分别以振幅和相位的形式加载在 SLM_1 和 SLM_2 上; 2) 用相干光照射 SLM_1 和 SLM_2, 经过 SLM_1 和 SLM_2 调制的相干光衍射传播至多重散射介质, 被其扰乱后, 在 CCD (charge coupled device) 上形成随机散斑场; 3) 利用 Sobel滤波器提取散斑的特征, 得到一个 16 × 16 的特征矩阵, 将其作为压缩函数的输出.

4 基于多重散射的光学 Hash 函数的构造

基于多重散射介质的光学 Hash 函数的构造过程主要可分为三个步骤: 消息预处理、数据压缩以及输出变换.

4.1 消息预处理

在进行数据压缩之前, 需要对原始消息进行预处理. 预处理操作如下: 1) 将消息数据长度用 64 bit 二进制数表示, 并作为附加信息添加到消息末尾; 2) 将 1) 中的数据划分为固定长度的子块数据, 若最后一个子块数据的长度未达到所要求的固定长度, 则需要在其末尾进行数据填充, 一般做法是在末尾直接填充 0 或 1[10]. 预处理的步骤 1) 一般被称为 MD 强化, 其目的是为了增强算法的抗碰撞性. 假设有两则不同数据长度的消息 A 和 B, A 满足分组要求无需进行填充, 而 B 需要在其末尾全部填充 0 或者 1. 消息 B 经过填充之后, 其数据分布可能与消息 A 相同, 因此, 经过同样的 Hash 函数之后得到相同的 Hash 值, 这就意味着产生了碰撞, 这将是一个严重的安全漏洞. 通过引入 MD 强化, 由于不同的消息其数据长度不同, 因此可避免碰撞的发生. 在步骤 2) 的消息分组中, 本方案将原始消息划分为长度为 2048 bit 的数据块, 并将每一数据块编码成 8 bit 量化精度的 16 × 16 的图像 $(M_1, M_2, \cdots, M_t)$. 此外, 压缩函数还需要一个初始输入 H_1, 本方案以原始消息长度作为种子, 利用伪随机数生成器生成 2048 bit 二进制伪随机数, 并将其编码成 8 bit 量化精度的 16 × 16 的图像 H_1, 其生成过程如图 3 所示.

4.2 数据压缩

经过消息预处理操作后, 得到了光学 Hash 函数的初始输入 H_1 以及多个消息子图 $(M_1, M_2, \cdots, M_t)$, 随后即可利用光学压缩函数对各消息子图 (分组消息) 进行压缩, 其流程图如图 4 所示. 步骤描述如下:

1) 用 PC 分别将 M_1 和 H_1 以纯振幅和纯相位的形式写入 SLM_1 和 SLM_2, 则光波的复振幅可表示为

$$C_1 = M_1 \exp\left(\mathrm{j}2\pi H_1\right); \tag{3}$$

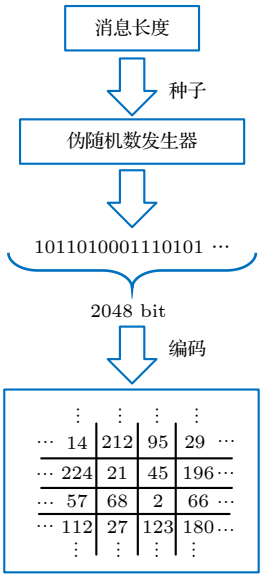

图 3 初始伪随机图像的生成

Fig. 3. Flowchart for creating initial pseudo-random image.

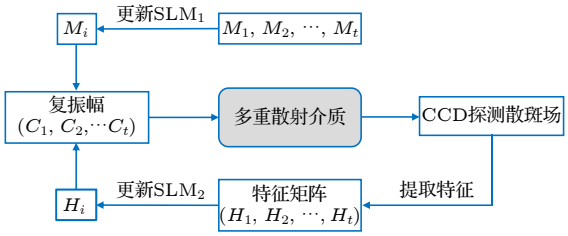

图 4 级联压缩流程图

Fig. 4. Flowchart of cascade compression.

2) 经过 SLM_1 和 SLM_2 调制后的相干光传输至 MSM 并与其相互作用, 最终在 CCD 上形成散斑图样, 散斑图样的强度表示为

$$I_1 = \left|\left[\left(C_1 * h_1\left(x, y, u\right)\right) \cdot P\right] * h_2\left(x, y, v\right)\right|^2, \tag{4}$$

其中

$$h_1\left(x, y, u\right) = \frac{\exp(\mathrm{j}2\pi u/\lambda)}{\mathrm{j}u\lambda} \exp\left[\frac{\mathrm{j}\pi}{u\lambda}\left(x^2 + y^2\right)\right], \tag{5}$$

$$h_2\left(x, y, v\right) = \frac{\exp(\mathrm{j}2\pi v/\lambda)}{\mathrm{j}v\lambda} \exp\left[\frac{\mathrm{j}\pi}{v\lambda}\left(x^2 + y^2\right)\right], \tag{6}$$

$h_1\left(x, y, u\right)$ 和 $h_2(x, y, v)$ 分别对应衍射距离为 u 和 v 的菲涅耳衍射的点扩散函数; u 和 v 分别表示 SLM_2 与 MSM 之间的距离以及 MSM 与 CCD 之间的距离; P 代表 MSM 的函数; *代表卷积运算符;

3) 利用 Sobel 滤波器提取散斑图样的特征, 得到量化精度为 8 bit 的 16 × 16 图像 H_2:

$$H_2 = \mathrm{extr}\left(I_1\right), \tag{7}$$

式中 $\mathrm{extr}\left(\cdot\right)$ 代表特征提取操作. 步骤 2) 和 3) 可用

压缩函数 $f(\cdot)$ 合并表示为

$$H_2 = f(M_1, H_1); \tag{8}$$

4) 将 M_2, , H_2 分别写入 SLM_1 和 SLM_2, 并重复步骤 2) 和 3), 得到下一个特征矩阵 H_3:

$$H_3 = f(M_2, H_2); \tag{9}$$

5) 同理, 对其他子图像重复步骤 1) — 3), 最终得到特征矩阵 H_{t+1}. 整个消息级联压缩过程如图 5 所示.

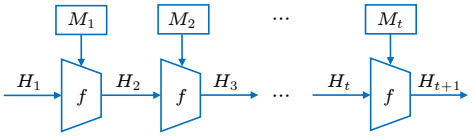

图 5 级联压缩过程

Fig. 5. Procedure of cascaded compression.

4.3 输出变换

在输出最终的 Hash 值之前, 还需要对压缩函数的最终输出 H_{t+1} 做输出变换. 本方案以 H_{t+1} 的均值作为阈值, 将 H_{t+1} 中大于或等于均值的像素灰度值设置为 1, 小于均值的像素灰度值设置为 0, 最后以逐行串接的形式将 H_{t+1} 中的值串联, 得到 256 bit 的 Hash 值.

5 仿真结果与分析

雪崩效应是评价 Hash 函数安全性能的重要指标[17], 其表明当输入消息产生微小变化时, 比如反转一个二进制位, 输出的 Hash 值将发生很大变化, 且依据严格雪崩准则, 当任何一个输入位发生变化时, 一个性能良好的 Hash 函数的 Hash 值至少有一半的位数发生变化[22]. 为了评估雪崩效应以及所提出光学 Hash 函数的稳定性, 拟采用以下几个参数[17,18]:

$$\mathrm{AEC}_{(i)} = \frac{1}{L}\sum_{k=1}^{L}|h_i(k) - h_i'(k)|, \tag{10}$$

$$\overline{\mathrm{AEC}} = \frac{1}{N}\sum_{i=1}^{N}\mathrm{AEC}_{(i)}, \tag{11}$$

$$\Delta B = \left[\frac{1}{N-1}\sum_{i=1}^{N}(AEC_{(i)} - \overline{AEC})^2\right]^{1/2}, \tag{12}$$

(10) 式中, h_i 和 h_i' 分别表示原始消息和将原始消息轻微改动后所对应的 Hash 函数; L 和 k 分别表示 Hash 值的总长度和比特位序数; $\mathrm{AEC}_{(i)}$ 表示第 i 次测试的雪崩系数. (11) 式中, $\overline{\mathrm{AEC}}$ 和 N 分别表示平均雪崩系数以及测试的总次数. 显然, 当 $\mathrm{AEC}_{(i)}$ 和 $\overline{\mathrm{AEC}}$ 的值越大时, 说明 Hash 函数的雪崩效应越强, 同时, 当标准差 ΔB 越小时, 说明 Hash 算法的稳定性越好.

数值仿真测试步骤如下: 1) 用所提出的光学 Hash 函数计算任意一个原始消息对应的 Hash 值; 2) 任意选取原始消息中的一位数据并对其进行修改, 计算消息被修改后的 Hash 值. 消息的具体修改过程如图 6 所示. 首先, 随机地选取图像中的任一像素, 如图 6 黑色圆圈所示; 随后提取该像素的像素值, 并通过二值化操作, 将该像素的像素值以二进制数的形式表示; 最后任意地选取这一像素值 (二进制表示) 的某一位执行数据的修改操作: 若该位的数据值为“1”, 则将其修改为“0”, 类似地, 若其值为“0”, 则将其修改为“1”; 3) 利用 (10) 式计算雪崩效应系数.

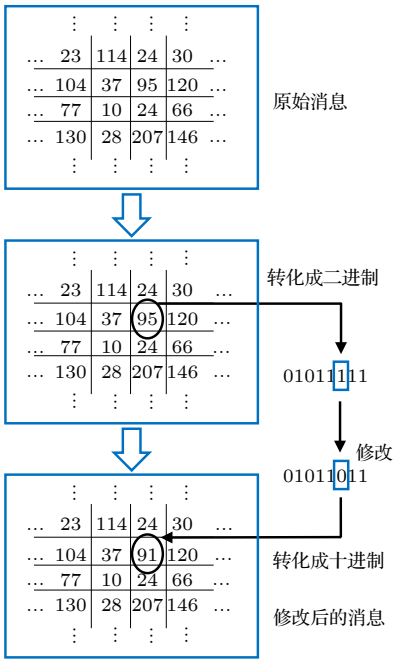

图 6 轻微修改原始消息的过程

Fig. 6. Flowchart of modifying the bit of message.

值得指出的是, 为了表征多重散射介质对于相干光 (振幅和相位) 的双重“混淆”和“扩散”作用, 仿真时选取 10 层相互间隔一定距离的随机相位掩模来表征多重散射介质, 间隔设置为 $z = 10$ mm, 如图 7 所示.

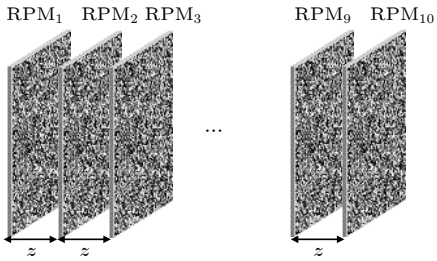

图 7 多重散射介质仿真模型

Fig. 7. Simulation model of the MSM.

重复上述步骤 2) 和步骤 3) 共 10000 次, 通过计算得到多个 $\mathrm{AEC}_{(i)}$ 值, 再结合 (11) 式以及 (12) 式可计算平均雪崩系数 $\overline{\mathrm{AEC}}$ 及标准差 ΔB, 利用这些参数可以评判一个 Hash 函数的性能优劣. 在仿真实验中, 分别对随机生成的 10, 100 和 1000 kbit 的原始消息进行测试, 测试结果如图 8 所示. 根据 (11) 式和 (12) 式计算平均雪崩系数 $\overline{\mathrm{AEC}}$ 及标准差 ΔB, 结果如表 1 所列. 为了进一步验证所提出的光学多重散射 Hash 函数的性能, 比较了本方案与传统的 MD5 和 SHA-1 的平均雪崩系数和稳定性数值, 相应的数值结果如表 2 所列.

测试结果表明, 对三组不同数据长度的消息而言, 在 10000 次的测试中, 任意改变原始消息中的某一位, 其对应的 Hash 值与原始消息的 Hash 值相比几乎一半的位数发生改变, 说明所提出的光学 Hash 函数具有良好的雪崩效应. 同时, 在测试结果中, 三组数各自的 ΔB 分别是 0.0770, 0.0647, 0.0636, 表明所提出的光学 Hash 函数具有较好的稳定性. 在测试过程中, 分别对三组不同长度的消息测试 10000 次, 并未出现一次碰撞, 即 $\mathrm{AEC}_{(i)} = 0$, 表明该 Hash 函数具有优秀的抗碰撞性. 进一步地, 通过对比可知, 本方法的雪崩效应系数与传统 Hash 函数 (MD5 和 SHA-1) 相当 (如表 2).

表 1 雪崩效应测试结果

Table 1. Results of testing avalanche effect.

	10 kbit	100 kbit	1000 kbit	平均值
$\overline{\mathrm{AEC}}$	0.49	0.50	0.50	0.50
ΔB	0.0770	0.0647	0.0636	0.0684

表 2 与 MD5 和 SHA-1 算法的比较

Table 2. Comparison with MD5 and SHA-1.

	本方案	MD5	SHA-1
$\overline{\mathrm{AEC}}$	0.50	0.50	0.50
ΔB	0.0684	0.0437	0.0392

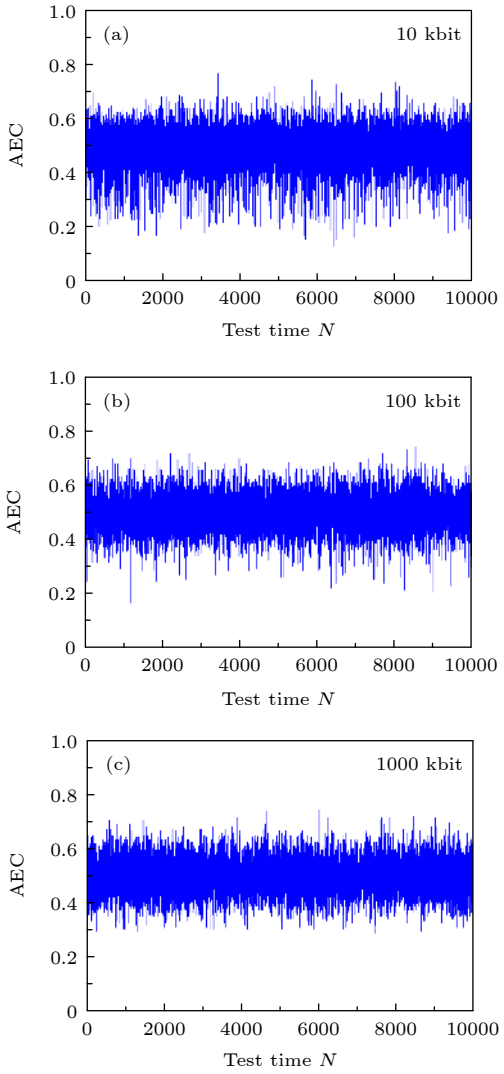

图 8 10000 次测试下的 AEC 分布, 消息长度为 (a) 10 kbit, (b) 100 kbit, (c) 1000 kbit

Fig. 8. Distribution of AEC values in tests for the messages with (a) 10 kbit, (b) 100 kbit, and (c) 1000 kbit.

6 总 结

本文提出了一种基于光与多重散射介质相互作用的光学 Hash 函数构造方法, 该光学 Hash 函数以多重散射介质为核心部件, 利用多重散射介质对调制光进行天然而随机的散射, 实现对输入信息的混淆和扩散作用, 同时, 结合 Sobel 滤波器进一步完成散射信号的特征提取, 最终实现了将任意长度的输入消息压缩为固定长度的输出 (Hash 值) 的目的. 相比于已报道的光学 Hash 函数, 该方法利用了散射介质对输入信号所具有的天然置乱特性, 提高了其光电混合实现的可行性. 数值仿真结果表明, 所设计的光学 Hash 函数具有优秀的雪崩

效应以及抗碰撞性, 与传统 Hash 函数的安全性能相当.

参考文献

[1] Schneier B, 1996 *Government Information Quarterly* **13** 336
[2] Refregier P, Javidi B 1995 *Opt. Lett.* **20** 767
[3] Liu F M, Zhai H C, Yang X P 2003 *Acta Phys. Sin.* **52** 2462 (in Chinese) [刘福民, 翟宏琛, 杨晓苹 2003 物理学报 **52** 2462]
[4] Situ G H, Zhang J J 2004 *Opt. Lett.* **29** 1584
[5] Javidi B, Carnicer A, Yamaguchi M , Nomura T, Pérez-Cabré E 2016 *J. Opt.* **18** 083001
[6] Carnicer A, Montes-Usategui M, Arcos S, Juvells I 2005 *Opt. Lett.* **30** 1644
[7] Peng X, Zhang P, Wei H, Yu B 2006 *Opt. Lett.* **31** 1044
[8] 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]
[9] Cheng X C, Cai L Z, Wang Y R, Meng X F, Zhang H, Xu X F, Shen X X, Dong G Y 2008 *Opt. Lett.* **33** 1575
[10] Liao M H, He W Q, Lu D J, Wu J C, Peng X 2017 *Opt. Laser. Eng.* **98** 34
[11] Peng X, Wei H Z, Zhang P 2006 *Opt. Lett.* **31** 3579
[12] Qin W, Peng X 2010 *Opt. Lett.* **35** 118
[13] Cai J J, Shen X J, Lei M, Lin C, Dou S F 2015 *Opt. Lett.* **40** 475
[14] Volodin B L, Kippelen B, Meerholz K, Javidi B, Peyghambarian N 1996 *Nature* **383** 58
[15] Wang X G, Chen W, Mei S T, Chen X D 2015 *Sci. Rep.* **5** 15668
[16] He J T, He W Q, Liao M H, Lu D J, Peng X 2017 *Acta Phys. Sin.* **66** 044202 (in Chinese) [何江涛, 何文奇, 廖美华, 卢大江, 彭翔 2017 物理学报 **66** 044202]
[17] Rivest R L 1991 *Lect. Notes. Comput. Sci.* **537** 303
[18] Rivest R L https://www.rfc-editor.org/rfc/rfc1321 [2020-9-10]
[19] He W Q, Peng X, Qin W, Meng X F 2010 *Opt. Commun.* **283** 2328
[20] He W Q, Peng X, Qi Y K, Meng X F, Qin W, Gao Z 2010 *Acta Phys. Sin.* **59** 1762 (in Chinese) [何文奇, 彭翔, 祁永坤, 孟祥锋, 秦琬, 高志 2010 物理学报 **59** 1762]
[21] Lai H, He W, Peng X 2013 *Appl. Opt.* **52** 6213
[22] Webster A F, Tavares S E 1986 *Lect. Notes. Comput. Sci.* **218** 523

Optical Hash function based on multiple scattering media*

He Wen-Qi Chen Jia-Yu Zhang Lian-Bin Lu Da-Jiang
Liao Mei-Hua† Peng Xiang‡

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

(Received 7 September 2020; revised manuscript received 5 November 2020)

Abstract

Hash functions, which can extract message digest from input messages as output, play an important role in digital signature and authentication. Meanwhile, Hash functions are essential in many cryptographic protocols and regimes. With the research becoming more and more in depth, a series of Hash functions is proposed, such as MD series and SHA series. At the same time, the security analysis and attacks against Hash functions are carried out. The security of Hash functions is threatened. In this case, how to improve the security of the Hash functions becomes the primary concern. In this paper, an optical Hash function based on the interaction between light and multiple scattering media is proposed. Unlike most of the traditional Hash functions which are based on mathematical transformations or complex logic operations, this method innovatively takes advantage of the natural random scattering effect of multiple scattering media on coherently modulated light, and realizes the "confusion" and "diffusion" of modulated light, which satisfies the core functional requirement of the Hash function: one-way encoding/encryption with strong security. The photoelectric hybrid system designed by this method can effectively simulate the "compression function" in the Hash function. Combined with the Sobel filter with feature extraction function, the input data of arbitrary length can be compressed and encrypted into the output with a fixed length of 256-bit (Hash value). The principle of the proposed optical Hash function can be described as follows. 1) Two 8-bit images with a size of 16×16 pixels are loaded in SLM_1 (amplitude-only spatial modulator) and SLM_2 (phase-only spatial modulator) respectively. 2) The coherent wavefront is modulated by SLM_1 and SLM_2, and then propagates on multiple scattering media. 3) A speckle pattern is recorded by CCD because of the confusion of multiple scattering media. 4) The features of the speckle pattern, which is extracted by Sobel filter, serve as the input of the next compression function. For the unpredicted and non-duplicated disorder multiple scattering media, it is tremendously difficult to determine the internal state of the multiple scattering media. Therefore, the proposed optical Hash function is considered to have a high security. A series of simulation results shows that the proposed optical Hash function has a good "avalanche effect" and "collision resistance", and its security performance is comparable to that of the most widely used traditional Hash functions (MD5 and SHA-1).

Keywords: optical information security, optical Hash function, multiple scattering media, avalanche effect

PACS: 42.30.Kq, 42.25.Dd, 42.25.Fx **DOI:** 10.7498/aps.70.20201492

* Project supported by the National Natural Science Foundation of China (Grant Nos. 61875129, 61705141, 61805152), the Sino-German Center for Research Promotion (Grant Nos. GZ1391, M-0044), and the Natural Science Foundation of Guangdong Province, China (Grant No. 2018A030310561).

† Corresponding author. E-mail: liaomeihua@outlook.com

‡ Corresponding author. E-mail: xpeng@szu.edu.cn