Optics Communications 283 (2010) 2328–2332

Contents lists available at ScienceDirect

Optics Communications

journal homepage: www.elsevier.com/locate/optcom

The keyed optical Hash function based on cascaded phase-truncated Fourier transforms

Wenqi He, Xiang Peng *, Wan Qin, Xiangfeng Meng

College of Optoelectronics Engineering, Shenzhen University, Key Laboratory of Optoelectronic Devices and Systems, Education Ministry of China, Shenzhen 518060, China

ARTICLE INFO

Article history:
Received 2 September 2009
Received in revised form 23 November 2009
Accepted 23 November 2009

Keywords:
Fourier optics
Optical system design
Hybrid systems
Image processing

ABSTRACT

An approach for constructing keyed optical Hash function (KOHF) is proposed, which is based on cascaded phase-truncated Fourier transforms (CPTFTs). The KOHF is created from a two-step one-way encryption process with a secret key imbedded. The non-linearity and one-way functionality is introduced by cascaded optical Fourier transforms with the phase-truncation operations, which could be implemented either digitally or optically. Once two 64-bit keyed Hash values are obtained in the two-step one-way encryption processes, respectively, they are then combined to form a final 128-bit keyed Hash value, which can also be regarded as a message authentication code (MAC). Moreover, the avalanche effect is also evaluated to show the performance of constructed KOHF with a set of numerical experiments.

1. Introduction

During the past decade the information security with optical technology has experienced a significant development due to the inherent advantages of parallel processing capability, multi-dimensional operation, and high security strength in optical signal processing [1,2]. However, most of the proposed optical security techniques, including optical encryption and optical watermarking, were built on a mechanism of symmetric cryptography. From the perspective of information security, the transmission and management of secret key is a problem remained to be solved in symmetric cryptography. In addition, in the framework of symmetric cryptography it would be hard to accomplish the tasks such as the check of message integrity and the identification of the legal users, which are all crucial issues of great concern if extending optical security to the applications under the network environment. Recently, some researchers have made a few attempts to address the issue of key distribution, in which they tried to combine an optical symmetric encryption algorithm with a non-optical asymmetric encryption strategy in order to ensure the security of key assignment [3–5]. Furthermore, an optically asymmetric encryption algorithm based on the principle of wavefront sensing has also been proposed [6] in attempt of optically generating two different keys in a cryptosystem, one for encryption and the other for decryption. However, all these approaches are preliminary and there are a number of problems yet to be solved in terms of optical asymmetric cryptography. For example, although the combination of optical symmetric encryption with non-optical asymmetric algorithm could be used to partly solve the problem of key distribution, it is still hard to cope with the issues such as the check of message integrity and the identification of legal users. In order to address these issues optically, it would be necessary to further explore the technique in the framework of optical asymmetric cryptography.

In this paper, we introduce a keyed optical Hash function (KOHF). A keyed Hash function can be useful for the check of message integrity and user identifications, both of which are significant in the applications of network security. The rest parts of this paper are organized as follows: Section 2 briefly introduces the basic concept of keyed Hash function. Section 3 describes how to construct a keyed optical Hash function in details. Section 4 presents computer simulations and validation of proposed keyed optical Hash function. Finally, the major points drawn from this approach are concluded in the final section.

2. Basic concept of keyed Hash function

As mentioned earlier, the check of the message integrity and the identification of legal users play an important role in information security. To check the message integrity, it usually needs to create a message digest MD (or Hash value). With the message digest one is able to identify whether or not the original message is integrated and if original message has been tampered. Mathematically, the creation of message digest mainly depends on so called one-way

* Corresponding author. Tel.: +86 755 26538548; fax: +86 755 26538580.
E-mail address: xpeng@szu.edu.cn (X. Peng).

0030-4018/$ - see front matter © 2009 Published by Elsevier B.V.
doi:10.1016/j.optcom.2009.11.060

function or Hash function [7], it was first introduced in early 1950s. Since then various Hash algorithms were designed, and extensively studied [8–13], in which the most widely used were MD5 [10] and SHA-1 [13], invented by Rivest in 1992 and the NIST in 1995 respectively. However, some kinds of collisions in these Hash schemes have been recently found by Wang, etc. [14]. All the Hash functions mentioned above were constructed based on pure mathematical theory. On the other hand, some Hash algorithms taking advantage of a physical phenomenon or process have been recently developed from the chaos theory [15]. A one-way Hash function can map an arbitrary-length message to a bit stream with fixed length. In order to further enhance the security, the Hash function usually works with an embedded key, and therefore named keyed Hash function [16]. While verifying the integrity of a message and the identity of the message sender simultaneously, a keyed Hash function is then required. Suppose that two parties communicate over an insecure channel, one party must verify the identity of his counterpart while he must also authenticate the integrity of the message sent to him. In this case, the party-A sends a message associated with a keyed Hash value, also referred to as a message authentication code, MAC, to party-B. The keyed Hash function works as a function of the transmitted message and together with a shared secret key. At the end of receiver, party-B recomputes the received message using the same keyed Hash function (and secret key) to generate another MAC′ and checks whether or not this MAC′ equal to the MAC attached to the received message. If only the attached keyed Hash value matches to the recomputed one, it can be verified that the received message has not been tampered or forged when transmitted from A to B. Otherwise, the integrity of transmitted message has already been intruded by a third party. From forementioned process, it can be seen that the keyed Hash function plays an important role in forming a security protocol between two parties for the verification and identification.

Turning back to the construction of keyed Hash function, we recognized that the problem can be attributed to the construction of an efficient one-way function with an embedded secret key shared by two parties in the generation process of message digest. This motivates our current approach to construct a KOHF, which will be described in details in the next section.

A keyed Hash function can convert an arbitrary-length message, M, and a secret key, K, into a fixed-length keyed Hash value, h, i.e., $h = H(M, K)$. The keyed Hash function should at least fulfill following four necessary conditions: (1) Given M and K, it is easy to compute h. (2) Given h and M, it is hard to compute K such that $H(M, K) = h$. (3) Given M and K, it is hard to find another message, M′, and another secret key, K', such that $H(M, K) = H(M', K')$. (4) A slightly change in M or K will result in prominent change in h, which is so called avalanche effect [7,17].

3. Construction of keyed optical Hash function

In this section, we present a method to optically construct a keyed Hash function. This method is based on the cascaded phase-truncated Fourier transforms (CPTFTs), in which the nonlinearity and one-way mechanism arises from the operation of phase-truncations. A password, an arbitrary-length random series of letters such as “shenzhen123”, is assigned and shared between the both parties before the practical communication occurs. Taking the password as a seed, we can generate a secret key by use of linear congruential generator. In our approach the KOHF is constructed from a two-step one-way encryption process together with an embedded secret key, which may be either implemented digitally or optically. One possible optical/digital hybrid configuration to implement the cascaded phase-truncated Fourier transforms is shown in Fig. 1. Prior to explaining how this hybrid system works, we need a pre-processing for the message to be encrypted and the shared password. First, we generate a 512-bit pseudo random series from a linear congruential generator with the password as a seed. Furthermore, we encode the pseudo random series to a sub-image with 8-bit (256 gray levels), referred to as secret key plane, M_0. Second, the message with arbitrary length can be divided into a number of data blocks with 512-bit length for each. The data block could be also encoded to an 8×8 sub-image with 8-bit (256 gray levels) referred to as information plane. Suppose that we have $512 \times N$ bit message and it is divided into N numbers of sub-image matrices (M_1, M_2, $\ldots$, M_N).

Now we explain how the first one-way encryption process can be achieved to create a 64-bit keyed Hash value, $hash_1$ with the use of forementioned secret key plane and N numbers of sub-image matrices. As shown in Fig. 1, the spatial light modulator SLM_1 is an amplitude-only (AO) modulation device while SLM_2 is a phase-only (PO) modulation device. By electronic addressing, we can first write M_0 and M_1 onto SLM_1 and SLM_2, respectively, so that M_0 is AO modulated whereas M_1 is PO modulated. Combining SLM_1 and SLM_2 leads to initial complex amplitude t_1, which can be written as

$$t_1 = M_0 \cdot \exp(j2\pi M_1/255) \tag{1}$$

This synthesized complex transmittance is then illuminated with a plane wave. A charge coupled device (CCD) camera with 12-bit quantized accuracy on the back focal-plane of the Fourier-transformation (FT) lens detects only the power spectrum of t_1 whereas the phase information is automatically truncated. We denote this process as PTFT [M_i, M_j], which is also regarded as a compression function because the phase part of the signal has been removed. Numerically we are able to quantize the power spectrum to 12-bit. Then the lower 8-bit-plane are chosen and stored as an intermediate result, H_1. This process can be mathematically expressed as

$$H_1 = Q_{12\to 8}\left\{|\mathrm{FT}(t_1)|^2\right\} \tag{2}$$

where FT (.) denotes the Fourier transform, $|\bullet|$ stands for taking modulus operation, and $|\bullet|^2$ can lead to the power spectrum of FT(.), $Q_{12\to 8}\{.\}$ is an operation of extracting the lower 8-bit-plane of quantized power spectrum with 12-bit gray levels. Eqs. (1) and (2) consist of a basic processing unit in the construction of the KOHF in our approach. Substituting Eq. (1) for Eq. (2) we have

$$H_1 = \mathrm{PTFT}[M_0, M_1] = Q_{12\to 8}\left\{|\mathrm{FT}[M_0 \cdot \exp(j2\pi M_1/255)]|^2\right\} \tag{3}$$

Now we update SLM_1 with AO modulation of the H_1, while update SLM_2 with the PO modulation of the M_2, making up a new complex amplitude, t_2 at input plane of Fig. 1, i.e.

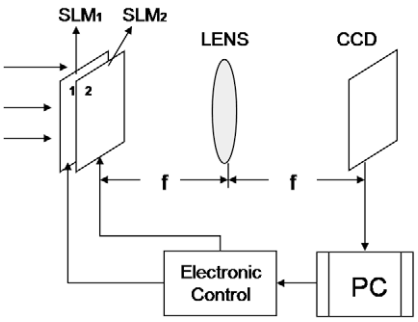

Fig. 1. Schematic diagram of keyed optical Hash function generator.