Optics Communications 428 (2018) 7–14

Contents lists available at ScienceDirect

Optics Communications

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

# An optical Hash function construction based on equal modulus decomposition for authentication verification

Avishek Kumar, Areeba Fatima, Naveen K. Nishchal *

*Department of Physics, Indian Institute of Technology Patna, Bihta 801 106, Patna, Bihar, India*

ARTICLE INFO

*Keywords:*
Hash function
Image encryption
Fractional Fourier transform
Joint transform correlator

ABSTRACT

This paper proposes a Hash based authentication scheme that employs equal modulus decomposition (EMD) and fractional joint transform correlator. An 8-bit grey scale image is separated into its constituent bit plane matrices. Each bit plane matrix is subjected to EMD encryption procedure employing numerically generated random phase mask (RPM) and amplitude mask (AM). The EMD encryption results into two complex functions, which are used for the generation of phase mask and amplitude mask for the next bit plane matrix. A two round EMD procedure is carried out to obtain an 8-bit intensity matrix which is Fourier transformed and its central frequency components are extracted to obtain a 256-bit Hash value. Numerical simulations have been carried out to validate the effectiveness and performance of the proposed scheme.

## 1. Introduction

Any activity on the internet is based on an exchange of data, which is binary in nature. The cryptographic algorithms heavily guard the data to ensure that it is received in the original form without any error. Apart from digital techniques, optical technology has been found useful in the area of information security [1]. Optical techniques usually enjoy large degrees of freedom and parallel processing architecture. Symmetrical optical image encryption schemes [2,3] have gained a lot of popularity and have been thoroughly explored by researchers. However, in the course of time, some vulnerability has been reported in symmetric cryptosystems [4–6]. To address the issue of linearity, optical asymmetric encryption methods were reported [7,8]. Peng et al. proposed an asymmetric image encryption scheme in which the decryption keys were derived during the encryption process employing amplitude- and phase truncation of Fourier spectrum [7]. Rajput and Nishchal reported a scheme in which asymmetric keys were used in the cryptosystem based on Fresnel domain encoding [8]. Despite of the good security features in the asymmetric cryptosystems based on Fourier transforms, it has been proved that they are vulnerable to special attack [9].

However, a question which remained to be answered was about the integrity of data and source authentication. A general solution of this problem is to obtain the digital signature of the data using Hash functions. A digital signature is a compressed form of the input data which is attached to the encrypted data while communicating. The receiver then detaches the digital signature, decrypts the data and rehashes it to obtain the digital signature. Data integrity and authenticity is restored if the digital signatures match perfectly [10–17].

A method to implement Hash function based on spatiotemporal chaos has been reported [10]. The message to be hashed was divided into fixed length data blocks. Each message block was then compressed using the proposed Hash function whose keys and initial conditions were derived from the data block. Further attempts to use chaos theory for implementing Hash functions have been reported [11–15]. However, they consumed considerable computational time and offered difficulty in practical implementation. A cascaded phase-truncated Fourier transform (CPTFT) based optical Hash function of 128-bit length Hash value has been reported in which a fixed password was used to generate a pseudo random series which was transformed into a secret key plane [16]. A block based cascading structure to obtain an optical Hash function has been implemented by dividing the input image equally into a number of blocks has been reported [17]. Utilizing the principle of two beam interference and phase truncation operation a 128-bit Hash value was obtained by initializing a pseudo random image. However, the schemes reported in Refs. [16,17] were prone to sensitivity issues and less secure because of the small bit length of the resultant Hash function. Elaborative security and performance analysis were not carried out. The system did not consider the issues related to noise which is an inherent problem in free space optical setup.

Cryptographic schemes applying the concept of coherent superposition and equal modulus decomposition (EMD) recently gained a lot of attention owing to its resistance to special attack [18–21]. Inspired by the

* Corresponding author.
*E-mail address:* nkn@iitp.ac.in (N.K. Nishchal).

https://doi.org/10.1016/j.optcom.2018.07.027
Received 1 March 2018; Received in revised form 21 May 2018; Accepted 9 July 2018

EMD methodology, an authentication verification scheme combining an optical Hash function and fractional joint transform correlator (FJTC) is presented in this paper [22–26]. An 8-bit grey scale image taken as input is separated into its constituent bit plane matrices. Each bit plane matrix is subjected to EMD encryption procedure employing numerically generated random phase mask (RPM) and amplitude mask (AM) with constant seed at the initial state. The output of the EMD operation results into two complex functions which are used for generation of RPM and AM respectively for the next bit plane matrix. Finally, the complex functions obtained after EMD operation on the 8-bit plane matrix are added and inverse Fourier transformed. Additive white Gaussian noise is added to the obtained spectra and recorded as an 8-bit intensity matrix. The recorded matrix is flipped upside down and the EMD encryption process is repeated to obtain another 8-bit intensity matrix which is Fourier transformed and the central frequency components are captured and recorded in an 8-bit format. This gives the 256-bit Hash value of the input image.

## 2. Principle.

### 2.1. The EMD methodology

An input image is bonded with an RPM and is Fourier transformed. The obtained complex spectrum is divided into two complex spectra with equal magnitude and different phases. One of the phases is termed as the cipher-text and the other is the cipher-key. During decryption, the phases are added together and inverse Fourier transformed. The absolute value of the obtained spectra gives the decrypted image [18]. Mathematically the EMD encryption may be represented as,

$$I(u,v) = FT\left\{\sqrt{f(x,y)}\exp[i2\pi r(x,y)]\right\} \tag{1}$$

Here, $f(x,y)$ is the intensity distribution of input image, $r(x,y)$ is a distribution of random values in the range [0, 1]. The complex spectrum represented in Eq. (1) is now phase-truncated (PT) and amplitude-truncated (AT).

$$P(u,v) = PT[I(u,v)] \tag{2}$$

$$A(u,v) = AT[I(u,v)] \tag{3}$$

The two phases, one serving as the cipher-text and the other serving as cipher-key may be mathematically represented as [18],

$$P_1(u,v) = \frac{A(u,v)/2}{\cos[P(u,v)-\theta(u,v)]}\exp[i\theta(u,v)] \tag{4}$$

$$P_2(u,v) = \frac{A(u,v)/2}{\cos[P(u,v)-\theta(u,v)]}\exp[i\{2P(u,v)-\theta(u,v)\}] \tag{5}$$

where, $\theta(u,v)$ is a distribution of random values in the interval $[0, 2\pi]$.

### 2.2. The construction of Hash function

Employing the EMD methodology, a Hash function construction is described. The $n$th bit-plane of an 8-bit grey scale image may be represented as $f_n(x,y)$. Initially, an RPM represented as $\xi_0(x,y) = \exp[i2\pi r(x,y)]$ is bonded to the first bit-plane of the image. The obtained function is Fourier transformed as,

$$\rho_n(u,v) = FT\{f_n(x,y)\xi_0(x,y)\} \tag{6}$$

The Eq. (6) is subjected to phase-truncation (PT) operation,

$$\phi_n(u,v) = PT[\rho_n(u,v)] \tag{7}$$

Eq. (6) is divided by Eq. (7) numerically and the resultant is amplitude-truncated (AT),

$$\sigma_n(u,v) = AT\left[\frac{\rho_n(u,v)}{\phi_n(u,v)}\right] \tag{8}$$

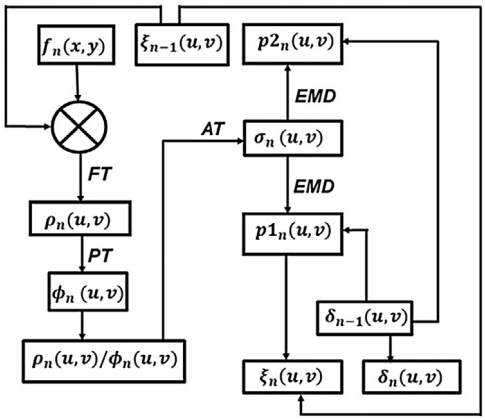


**Fig. 1.** A flowchart of the Hash function construction as described by the series of mathematical expressions in Section 2.2. The rectangular boxes represent the value of the functions before and after a mathematical operation. The double-crossed circle represents a multiplication operation. The arrow symbols make available the value of the function for the next mathematical operation. FT: Fourier transform, PT: phase truncation, AT: amplitude truncation, EMD: equal modulus decomposition.

An initial AM represented as $\delta_0(u,v) = [2\pi n(u,v)]$, where $n(u,v)$ is a distribution of random values in the range [0, 1] is used along with the function represented in Eq. (8) to obtain two complex phases which may be given as [18,19],

$$P_{1n}(u,v) = \frac{\phi_n(u,v)}{2\cos[\sigma_n(u,v)-\partial_{n-1}(u,v)]}\exp[i\sigma_n(u,v)] \tag{9}$$

$$P_{2n}(u,v) = \frac{\phi_n(u,v)}{2\cos[\sigma_n(u,v)-\partial_{n-1}(u,v)]}\times\exp[i\{2\sigma_n(u,v)-\partial_{n-1}(u,v)\}] \tag{10}$$

These phase functions are numerically obtained and are used to generate RPM and AM to be used for the next bit-plane of the image. The phase mask may be represented as,

$$\xi_n(u,v) = norm\left[P_{1n}(u,v)\xi_{n-1}(u,v)\right] \tag{11}$$

Similarly, the AM may be represented as,

$$\delta_n(u,v) = norm\left[P_{2n}(u,v)\delta_{n-1}(u,v)\right] \tag{12}$$

Here, *norm* represents normalization operation, which is numerically applied to the function. Finally, for the 8-bit plane, the phase functions are added and inverse Fourier transformed (IFT)

$$\alpha_8(x,y) = IFT\left[\xi_8(u,v)+\delta_8(u,v)\right] \tag{13}$$

Numerically generated additive white Gaussian noise (AWGN) with constant seed is added to the function obtained in Eq. (13).

$$\beta_8(x,y) = [\left[\alpha_8(x,y)\right] + AWGN] \tag{14}$$

The function is recovered as an 8-bit intensity matrix, we may denote it as $g_1(x,y)$. This matrix is flipped upside down and separated into its constituent bit-planes numerically to repeat the procedure. The 8-bit intensity matrix obtained now may be denoted as $g_2(x,y)$. This matrix is compressed to obtain the Hash function. The block diagram of the Hash function construction is shown in Fig. 1. To perform compression, the function $g_2(x,y)$ is Fourier transformed,

$$h(u,v) = FT\left[g_2(x,y)\right] \tag{15}$$

The central region of the matrix $h(u,v)$ is extracted as an $8\times4$ matrix. This matrix is termed as the 256-bit Hash value of the input image. We may represent the Hash operation as [16,17],

$$H = Hash\left[f_n(x,y)\right] \tag{16}$$