Optics & Laser Technology 88 (2017) 111–120

Contents lists available at ScienceDirect

Optics & Laser Technology

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

Full length article

Image authentication based on double-image encryption and partial phase decryption in nonseparable fractional Fourier domain

Lin Yuan[a,b,*], Qiwen Ran[a,c], Tieyu Zhao[a]

[a] State Key Laboratory of Tunable Laser Technology Research, Institute of Optic-Electronics, Harbin Institute of Technology, Harbin, 150001 China
[b] College of Mathematics, Physics and Information Engineering, Zhejiang Normal University, Jinhua, 321004 China
[c] Nature Science Research Center of Science and Technology, Harbin Institute of Technology, Harbin, 150001 China

ARTICLE INFO

Keywords:
Double-image encryption
Nonseparable fractional Fourier transform
Image authentication
Nonlinear correlation algorithm

ABSTRACT

In this paper an image authentication scheme is proposed based on double-image encryption and partial phase decryption in nonseparable Fractional Fourier transform domain. Two original images are combined and transformed into the nonseparable fractional Fourier domain. Only part of the phase information of the encrypted result is kept for decryption while the rest part of phase and all the amplitude information are discarded. The two recovered images are hardly recognized by visual inspection but can be authenticated by the nonlinear correlation algorithm. The numerical simulations demonstrate the viability and validity of the proposed image authentication scheme.

1. Introduction

In past decades, the optical image encryption techniques have been widely studied due to its advantage of potential fast computational processing and the parallelism achievable. The double random phase encoding (DRPE) [1–4] is a classical method among various optical encryption techniques. However, it has been testified that under certain conditions DRPE is vulnerable to some kinds of attacks [5–10]. Although the probability of being broken decreases by using iterative random phase encoding, the computation and storage costs increase simultaneously. Other than DRPE, multiple-image encryption has been proposed later and developed considerably for its convenience of encrypting multiple images at the same time and its applicability to color images [11–15]. In recent years, many different optical transforms have been employed in image encryption schemes, such as gyrator transform (GT) [16–19], fractional Fourier transform (FRFT) [20–23], nonseparable fractional Fourier transform (NFRFT) [24,25]. One of advantages of NFRFT is that it cannot be expressed as a tensor product of two one-dimensional transforms neither in the space domain nor in the Wigner space-frequency domain. Therefore, it adequately mixes the information of the signal not only inside each dimension but also between two dimensions [24]. When used in encryption, it enhances the security level of the cryptosystem. In this paper, an image authentication scheme is proposed based on double-image encryption and partial phase decryption in NFRFT domain. Two original images are respectively taken as the real and imaginary part of the input signal. Perform NFRFT on the input signal with the transform order and the coefficient parameters as encryption keys. Not all the encrypted data are kept for decryption but merely partial phase information. The rest phase information and the whole amplitude information of the encrypted result are discarded so as to reduce the costs of transmission and storage. Due to being decrypted from only partial phase information, the two recovered images cannot be identified by naked eyes but can be verified by means of correlation algorithms [26–31] among which we chose the nonlinear correlation algorithm as our tool. One of the advantages of the proposed double-image authentication scheme is that it is capable of authenticating two images using only one encryption-decryption process. To our knowledge, the authentication technique is proposed for the first time that can achieve two respective images authentications only by a single encryption-decryption operation.

The rest of the paper is organized as follows. Section 2 presents the details of the proposed image authentication scheme. Section 3 gives the numerical simulations and results to demonstrate the performance and verify the validity of the proposed scheme. The conclusion is drawn and stated in the final section.

2. Image authentication based on double-image encryption and partial phase decryption in NFRFT domain

2.1. Double-image encryption in NFRFT domain

We first recall the knowledge of NFRFT. NFRFT with transform order α is mathematically defined as [24].

[*] Corresponding author at: College of Mathematics, Physics and Information Engineering, Zhejiang Normal University, Jinhua 321004, China.
E-mail address: ylin2002@126.com (L. Yuan).

http://dx.doi.org/10.1016/j.optlastec.2016.09.004
Received 22 June 2016; Received in revised form 31 July 2016; Accepted 8 September 2016

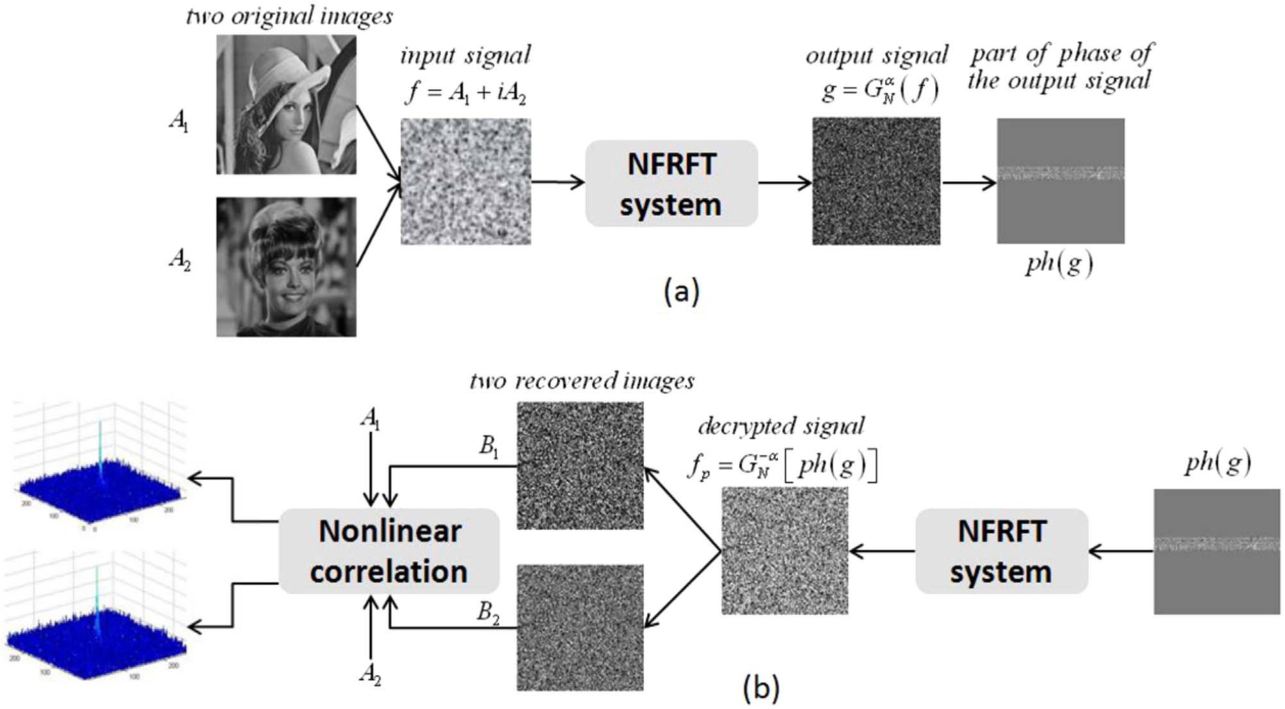

Fig. 1. The flowchart of the encryption and decryption-authentication. (a) The encryption process, (b) the decryption and authentication based on partial phase of encrypted image.

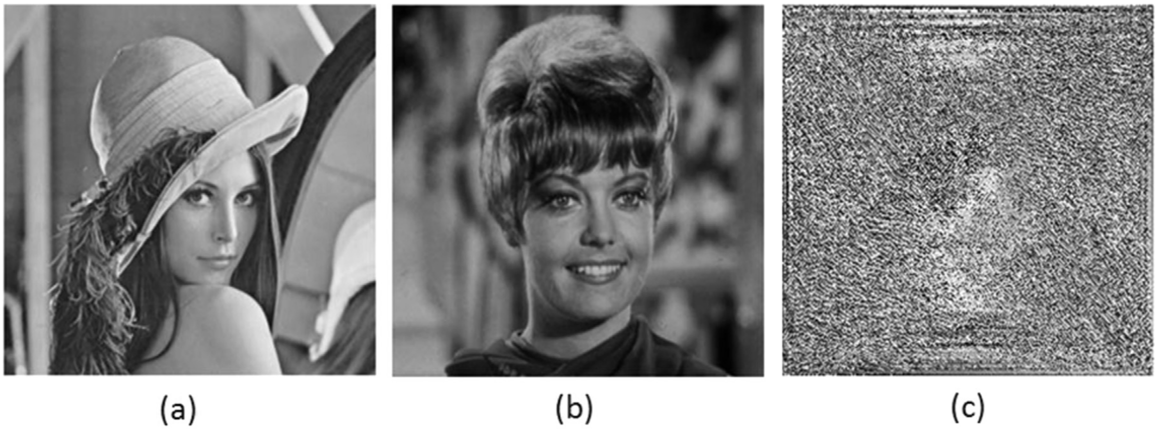

Fig. 2. The two original images. (a) ‘Lena’, (b) ‘Zelda’, (c) the phase of the encrypted result.

$$\left(G_N^{\alpha} f\right)\left(\mathbf{r}_o\right) = \frac{1}{4}\sum_{k=0}^{3}\sum_{l=0}^{3}\exp\left\{-\frac{i\pi}{2}\left[\left(\alpha - k\right)l\right] + \alpha i r_l\right\} f_k\left(\mathbf{r}_o\right). \tag{1}$$

where $f_0(\mathbf{r}_o)$=$f(x_o, y_o)$, $f_1(\mathbf{r}_o)$=$F(y_o, x_o)$, $f_2(\mathbf{r}_o)$=$f(-x_o, -y_o)$, $f_3(\mathbf{r}_o)$ =$F^3(y_o, x_o)$ are four basic functions and r_l, l=0,1,2,3 are any real numbers. $F(y_o, x_o)$ is the transposed Fourier transform of $f(x_i, y_i)$ and $\mathbf{r}_{i,o}$=$(x_{i,o}, y_{i,o})$ represent the input/output coordinates respectively. NFRFT has many common properties like FRFT and GT such as additive, unitary, etc. But unlike FRFT and GT, it is not periodic and does not belong to the class of linear canonical transforms (LCTs). The transform can be implemented by a photoelectric setup. The detailed description of the configuration of the setup is given in [24,25].

Two original images taken as the real or imaginary part respectively combine into a complex function (input signal). Performing the NFRFT on the input signal leads to the output signal (another complex function) in NFRFT domain. In the encryption system, the transform order and the coefficient parameters serve as secret keys. The flowchart of the encryption process is shown in Fig. 1(a). In classical cryptosystems, the recovering of the original image is to decrypt the whole encoded data. Such regular practice needs more transmission and storage costs on one hand and on the other hand causes security deficiency. To avoid these imperfections, in the proposed scheme, only partial phase of the encoded data is reserved for decryption. The two recovered images cannot reveal any useful visual information thereby enhance the security level of the cryptosystem.

2.2. Double-image authentication based on partial phase

First, selecting partial phase information of the output signal g to construct a new signal pH(g) which is then decoded with all the correct keys. Due to not all the encoded data involving in the decryption, the recovered images are hardly recognized by naked eyes. In order to