Optics and Lasers in Engineering 88 (2017) 20–27

Contents lists available at ScienceDirect

Optics and Lasers in Engineering

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

Cascaded Fresnel holographic image encryption scheme based on a constrained optimization algorithm and Henon map

Yonggang Su [a], Chen Tang [a,*], Xia Chen [a], Biyuan Li [a], Wenjun Xu [a], Zhenkun Lei [b]

[a] School of Electronic Information Engineering, Tianjin University, Tianjin, 300072 PR China
[b] State Key Laboratory of Structural Analysis for Industrial Equipment, Dalian University of Technology, Dalian, 116024 PR China

ARTICLE INFO

Article history:
Received 19 April 2016
Received in revised form
15 June 2016
Accepted 23 July 2016

Keywords:
Image/video encryption
Chaotic phase masks
Henon map
Cascaded Fresnel transform
Digital holography

ABSTRACT

We propose an image encryption scheme using chaotic phase masks and cascaded Fresnel transform holography based on a constrained optimization algorithm. In the proposed encryption scheme, the chaotic phase masks are generated by Henon map, and the initial conditions and parameters of Henon map serve as the main secret keys during the encryption and decryption process. With the help of multiple chaotic phase masks, the original image can be encrypted into the form of a hologram. The constrained optimization algorithm makes it possible to retrieve the original image from only single frame hologram. The use of chaotic phase masks makes the key management and transmission become very convenient. In addition, the geometric parameters of optical system serve as the additional keys, which can improve the security level of the proposed scheme. Comprehensive security analysis performed on the proposed encryption scheme demonstrates that the scheme has high resistance against various potential attacks. Moreover, the proposed encryption scheme can be used to encrypt video information. And simulations performed on a video in AVI format have also verified the feasibility of the scheme for video encryption.

1. Introduction

With the rapid development of computer and Internet technologies, the unauthorized distribution of data has become a serious problem, and both information security and intellectual property protection are of great concern. This has led to the extensive study of data encryption, digital signature, authentication, and watermarking methods. Among various existing technologies for data encryption, optical encryption techniques have attracted significant interest as they possess superior advantages such as high computation speed, high parallelism in applications and arbitrary parameter selection [1]. Refregier and Javidi firstly proposed the double random phase encoding (DRPE) architecture based on a 4-f optical system to encrypt the primary image into stationary white noise [2]. This pioneering achievement opened new fields of research in optical image encryption, and has paved the way for numbers of optical security and encryption systems subsequently proposed. However, optical DRPE scheme has been found to be vulnerable to some attacks, such as the known plaintext attack [3] and the chosen ciphertext attack [4]. In addition, the management and transmission of secret keys in optical DRPE cryptosystem are very inconvenient, because the whole random phase mask keys with the same size of encrypted image have to be sent to the authorized receiver side to decrypt the original image. There have been many strategies proposed to solve the above-mentioned problems. To enlarge the key space and enhance the security of DRPE, different optical domains such as the fractional Fourier transform (FrFT) domain [5–8] and the Fresnel transform (FrT) domain [9–11] have been employed. In these optical DRPE systems, the fractional transform orders and Fresnel transform distances are introduced as additional keys, which provide additional difficulties for the attackers of the system. Some more complex optical systems such as the multichannel fractional Fourier transform system [12], the multistage fractional Fourier transform system [13], the cascaded fractional Fourier transform system [14] and the cascaded Fresnel transform system combined with projection onto convex sets (POCS) algorithm [15] have also been employed to further enhance the security. To facilitate the management and transmission of secret keys in cryptosystems based on DRPE, some chaos-based image scrambling and encoding strategies have been developed and employed [16–18]. In these encryption strategies, the random phase masks are generated by chaotic maps, such as the Logistic map [16,17] and the tent map [18]. The initial values and control parameters of chaotic maps serve as secret keys, which makes the key management and transmission become very convenient. In addition, it is

* Corresponding author.
E-mail address: tangchen@tju.edu.cn (C. Tang).

http://dx.doi.org/10.1016/j.optlaseng.2016.07.012
0143-8166/

worth mentioning that some optical technologies, such as the digital holography [19–23], can provide a convenient form of recording the complex encrypted images after passing through the optical DRPE systems. In digital holography, phase-shifting techniques [19–21] are commonly used to retrieve the original complex information. However, these techniques need at least two interferograms to reconstruct the original complex object field. Unlike the phase-shifting techniques, the constrained optimization algorithm in digital holography [23] makes it possible to retrieve the original complex information from only single frame hologram. Nevertheless, owing to the high coherence of laser, the reconstructed image of digital holography will inevitably be influenced by the speckle noise. Besides, the limited resolution of CCD camera will also degrade the quality of the reconstructed image.

From the above reviews, embedding the DRPE into a more complex optical system may be an effective practice strategy to enhance the security. In addition, the practice of generating the random phase masks by chaotic maps can efficiently facilitate the management and transmission of secret keys in optical DRPE systems. However, among most existing chaos-based image encoding strategies, as mentioned above, the 1-D chaotic maps are commonly used to generate the random phase masks. There are some drawbacks such as small key space and weak security [24] existed in these cryptosystems. To solve these drawbacks, a realistic strategy is that use high dimensional chaos with complex dynamic characteristics rather than the 1-D chaotic maps to encode images.

In this paper, we propose a cascaded Fresnel holographic image encryption scheme based on a constrained optimization algorithm [23] and a two-dimensional (2-D) chaotic map. In the proposed encryption scheme, the random phase masks are generated by Henon map [25]. With the help of multiple chaotic phase masks, the original image can be encrypted into a noise-like image stored as the form of a hologram. To decrypt the image, the constrained optimization algorithm makes it possible to retrieve the original image from only single frame hologram. The Henon map, which is a well-known 2-D discrete-time dynamical system, owns complex dynamic characteristic and can provide more security for image encryption compared to 1-D chaotic maps. The strategy that the initial values and control parameters of Henon map serve as the main keys while the multiple axial distances and incident wavelength serve as the additional keys makes the key management and transmission become very convenient in our encryption scheme. Furthermore, the introduction of the constrained optimization algorithm makes the proposed encryption scheme can also be used for video encryption. Simulations performed on the images and video have demonstrated the security and validity of the proposed encryption scheme.

The rest of this paper is organized as follows. In the next section, the proposed encryption scheme will be described in detail. Results and security analyses are presented in Section 3, while conclusions will be drawn in the last section.

2. The proposed encryption scheme

Prior to the description of the proposed encryption scheme, we firstly present some preparative theories of chaotic Henon's system.

2.1. Henon map

The Henon map is a well-known 2-D discrete-time dynamical system, and is defined by

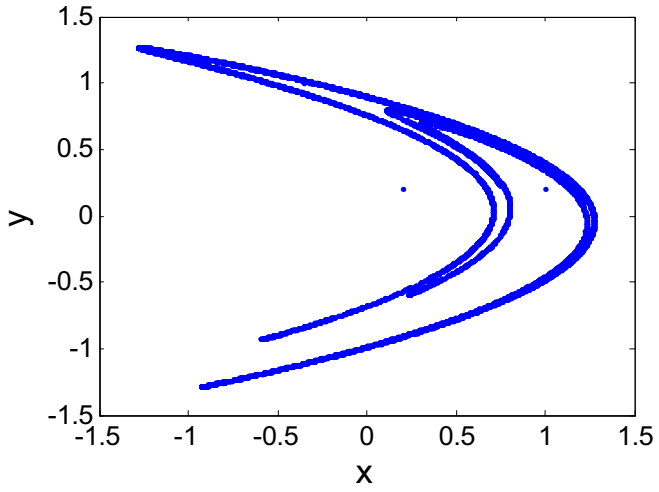

Fig. 1. Attractor of Henon map.

$$\begin{cases} x_{n+1} = 1 - \alpha x_n^2 + y_n \\ y_{n+1} = \beta x_n \end{cases} \quad (1)$$

The map depends on two control parameters, α and β, which for the classical Henon map have values of $\alpha = 1.4$ and $\beta = 0.3$. For the classical values the Henon map is chaotic, and for other values of α and β the map may be chaotic. The initial values x_0, y_0 and control parameters α, β can be used as secret keys. The attractor of Henon map is shown in Fig. 1 with the control parameters $\alpha = 1.4$, $\beta = 0.3$ and the initial values $x_0 = 0$, $y_0 = 0$.

With each iteration of the Henon map, two chaotic state variables x and y will be generated simultaneously. Suppose that the plain image is with the size $M \times N$, the Henon map will be iterated $M \times N$ times, and hence a series of x and y are generated. These random series will be used to generate the chaotic phase masks in the encryption and decryption process of the proposed encryption scheme.

2.2. Encryption algorithm

In this section, an image encryption scheme which combines the cascaded Fresnel transform holography and chaotic phase masks is proposed. To illustrate the proposed encryption algorithm, an experimental system which consists of a Mach–Zehnder interferometer, as shown Fig. 2, is employed. The lower arm of the interferometer is the optical path of the image encryption. The upper arm is the reference wave. A collimated plane wave is generated to illuminate an input image (i.e., original image), and

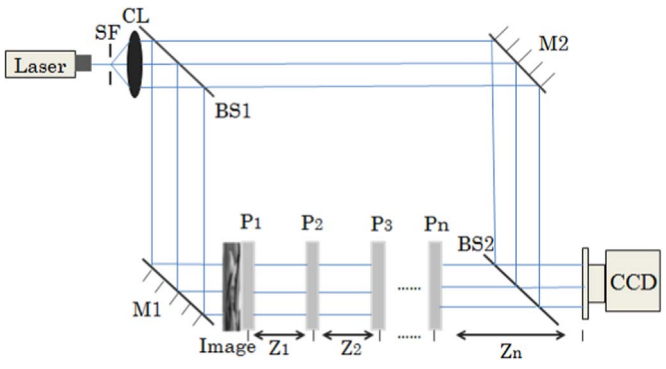

Fig. 2. Optical experiment setup for the proposed cryptosystem. SF: spatial filter; CL: collimating lens; BSs: beam splitters; Ms: mirrors; Ps: chaotic phase masks; Zs: Fresnel transform distances.