Optics Communications 380 (2016) 387–393

Contents lists available at ScienceDirect

Optics Communications

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

Three-dimensional information hierarchical encryption based on computer-generated holograms

Dezhao Kong [a,b], Xueju Shen [a], Liangcai Cao [b,*], Hao Zhang [b], Song Zong [b], Guofan Jin [b]

[a] Department of Electronic and Optics, Shijiazhuang Mechanical Engineer College, Shijiazhuang 050003, China
[b] State Key Laboratory of Precision Measurement Technology and Instruments, Tsinghua University, Beijing 100084, China

ARTICLE INFO

Article history:
Received 28 April 2016
Received in revised form
6 June 2016
Accepted 13 June 2016
Available online 22 June 2016

Keywords:
Holography
Optical encryption
Computer-generated hologram
Chaotic sequence

ABSTRACT

A novel approach for encrypting three-dimensional (3-D) scene information hierarchically based on computer-generated holograms (CGHs) is proposed. The CGHs of the layer-oriented 3-D scene information are produced by angular-spectrum propagation algorithm at different depths. All the CGHs are then modulated by different chaotic random phase masks generated by the logistic map. Hierarchical encryption encoding is applied when all the CGHs are accumulated one by one, and the reconstructed volume of the 3-D scene information depends on permissions of different users. The chaotic random phase masks could be encoded into several parameters of the chaotic sequences to simplify the transmission and preservation of the keys. Optical experiments verify the proposed method and numerical simulations show the high key sensitivity, high security, and application flexibility of the method.

1. Introduction

The conflict between information exchange and information security is considerably increasing, explaining why efforts are being devoted to data encryption and secure transmission recently. Information security with optical means has demonstrated that optical technology possesses several unique characteristics for securing information compared with its electronic counterpart, such as many degrees of freedom, optical computing and high parallelism [1–10]. Encryption of two-dimensional (2-D) information has been extensively studied in recent years since Refregier and Javidi proposed the double-random phase encoding technique [1]. Researchers have proposed various optical methods for image encryption based on different domains such as fractional Fourier transform domain [2–5], Fresnel transform domain [6–9] and Gyrator transform domain [10,11].

The chaotic maps have demonstrated great potential for information security, especially for image encryption. With a chaotic map, large number of random iterative values with the desirable properties of non-correlation, pseudo-randomness, and periodicity can be generated. Three types of chaos functions, including the logistic map, the tent map and the Kaplan-Yorke map, were involved to encrypt images, by generating chaotic random phase masks [10,12,13] and scrambling the encrypted images [14–16]. A coupled two-dimensional piece wise nonlinear chaotic map was also developed to overcome fundamental drawbacks of the one-dimensional chaotic system such as small key space and weak security [17].

Compared to the conventional 2-D information display, the three-dimensional (3-D) information is superior since it has the potential to accurately render sensations of depth, locations, and spatial relationships of the 3-D scenes information. Hence the development of 3-D display and information encryption would hugely benefit the visualization and security of multidimensional data, such as medical imaging and virtual reality [18–20]. Holographic 3-D display [21–24] provides realistic images without special eyewear. With the development of spatial light modulators and computing technology, the 3-D display based on computer-generated holograms (CGH) can now be displayed in real time [24–27].

Three-dimensional information encryption, different from the traditional 2-D image encryption, can improve the efficiency of information storage, transmission, display and encryption [28–32]. Some valuable works have been done about the 3-D information encryption with different methods, such as diffractive imaging [28], digital holography (DH) [18,29–31], integral imaging [32]. By contrast, the encryption based on CGHs has the advantages of easier preservation, transmission, and reconstruction for both real and virtual 3-D scenes, which can benefit the flexibility of 3-D information encryption.

In this paper, we propose a hierarchical encryption method for encrypting 3-D scenes information based on chaotic sequences and computer generated-hologram. The 3-D information is sliced into multiple layers, which are encoded into CGHs of the same

* Corresponding author.
E-mail address: clc@tsinghua.edu.cn (L. Cao).

http://dx.doi.org/10.1016/j.optcom.2016.06.037
0030-4018/

number primarily by angular spectrum propagation algorithm. Then the hierarchical encryption images and multiple-group keys are achieved by the mathematic hierarchical encoding (MHE) and chaotic sequences based on the logistic map. The chaotic random phase masks (CRPM) achieved by the logistic map are creatively applied in the generation of encrypted CGHs. All groups of keys such as logistic map parameters could be encoded into one quick response (QR) code for convenient passing. For the hierarchical encryption of 3-D scenes, the available amount of the decrypted 3-D information depends on different user's authority. Compared to 3-D information encryption by DH, complexity of obtaining key of proposed method is reduced and key accuracy is improved. The system is also robust to blind decryptions without knowing the correct propagation distance, wavelength, and phase keys used in the encryption.

2. Principle of the scheme

2.1. Chaos theory

Chaos theory is an evolutionary theory, which indicates that the nonlinear dynamical systems change from ordered state to disordered state. The dynamical systems can be described by various chaos functions, which are very sensitive to the initial parameters. The one-dimensional nonlinear chaos function logistic map is defined as

$$a_{n+1} = ra_n(1 - a_n) \tag{1}$$

where $a_n \in [0, 1]$ is random iterative values, a_0 is the initial value, and r denotes a mathematic parameter. When $r \in [3.5699456, 4]$, the logistic map will work at a chaotic state. The slight variations of the initial value will yield dramatically different random iterative values which form a non-periodic and non-converging sequence, as is shown in Fig. 1.

2.2. The encoding of 3-D scenes information by angular spectrum

The algorithm for 3-D scenes information CGHs is shown in Fig. 2. The 3-D model $O(\xi, \eta, z)$ is divided into K parallel layers with depth cues. The 2-D image in one layer can be denoted as $A_l(\xi_l, \eta_l)$, where $l=1, 2, 3, \ldots, K$. Then the lth layer $A_l(\xi_l, \eta_l)$ is encoded by the two-dimensional random pahse $\varphi_l(\xi_l, \eta_l)$. The random phase distribution added on the amplituede information is to simulate the diffusive effect of the object surface [33]. With the angular spectrum propagation algorithm, the phase distribution of the corresponding hologram of the l_{th} layer is,

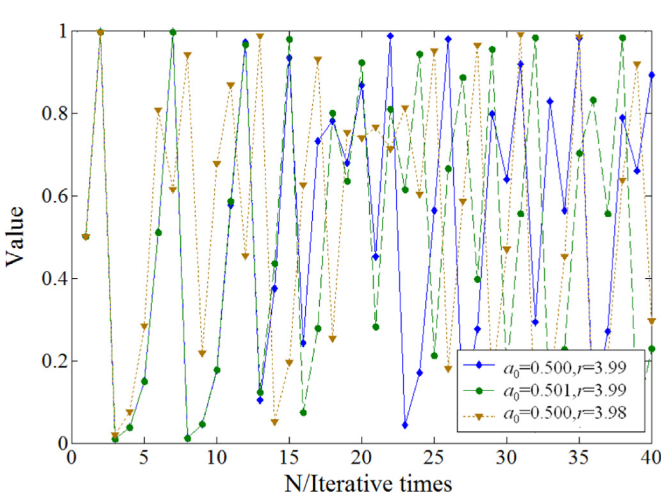

Fig. 1. Sensitivity of the logistic map on the initial values a_0 and r.

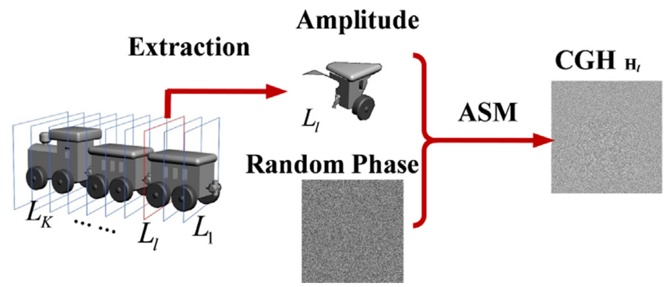

Fig. 2. The calculation of the CGH H_l. ASM, angular spectrum method.

$$H_l(x, y) = Ang\left\{ \boldsymbol{F}^{-1}\left\{ \boldsymbol{F}\left\{ A_l(\xi_l, \eta_l)\cdot \exp\left[j\varphi_l(\xi_l, \eta_l) \right] \right\} \exp\left[jkz_l\sqrt{1 - \lambda^2 f_\xi^{\,2} - \lambda^2 f_\eta^{\,2}} \right] \right\} \right\} \tag{2}$$

where $Ang(\ldots)$ denotes the operation of capturing phase, (x, y) is the hologram coordinate, (ξ_l, η_l) is the lth layer coordinate, (f_ξ, f_η) are spatial frequency, $k = 2\pi/\lambda$ is the wave number in free space, z_l is the propagation distance from the lth layer to the hologram, F and F^{-1} denote Fourier transform and inverse Fourier transform, respectively [33].

2.3. The encryption and decryption algorithm

In order to achieve the encryption of 3-D scenes information, the encryption process can be divided into two parts, generation of CRPM and MHE. The logistic map is applied to generate CRPM. Two-dimensional logistic map is expressed as

$$\begin{cases} a_{i+1} = r_a a_i(1 - a_i) \\ b_{i+1} = r_b b_i(1 - b_i) \end{cases} \quad (0 \le i \le h) \tag{3}$$

where initial values a_0, $b_0 \in [0,1]$ and parameter r_a, $r_b \in [3.5699456,4]$, $h = M \times N$ denotes the size of image, a_{i+1} and b_{i+1} denote the random iterative values. With different initial values a_0, b_0 and parameter r_a, r_b, non-periodic and non-converging random sequences $X=\{a_0, a_1, a_2, \ldots, a_i, \ldots, a_h\}$ and $Y=\{b_0, b_1, b_2, \ldots, b_i, \ldots, b_h\}$ can be generated iteratively.

Every element $C_l(x_i, y_i)$ of the l_{th} two-dimensional CRPM $C_l(x, y)$, achieved by logistic map, can be expressed as

$$C_l(x_i, y_i) = \exp\left[j\pi(a_i + b_i) \right] \text{ where } \left(\begin{array}{l} x_i = \begin{cases} \text{mod}(i, M) & (\text{mod}(i, M) \neq 0) \\ M & (\text{mod}(i, M) = 0) \end{cases} \\ y_i = ceil(i/M) \end{array} \right) \tag{4}$$

where $1 \le i \le h$, mod(…) denotes operation of mod and ceil(…) denotes operation of ceiling, a_i and b_i belong to non-periodic and non-converging random sequences X and Y. So the l_{th} random phase mask $C_l(x, y)$ could be decided and expressed by the logistic map with certain initial values a_0, b_0 and parameter r_a, r_b.

Hologram distributions $H_l(x,y)$ of the lth layer and CRPM $C_l(x, y)$ are calculated. The MHE is described as shown in Fig. 3. When the first CRPM $C_1(x,y)$ is used to encode the CGH $H_1(x,y)$, the encrypted CGH $H_{E1}(x,y)$ of $H_1(x,y)$ is achieved as

$$H_{E1}(x, y) = H_1(x, y)\cdot C_1(x, y) + \alpha_1 C_0(x, y) \tag{5}$$

where $C_0(x,y)$ denotes initial CRPM, α_1 denotes the encoding factor. Define the l_{th} encrypted CGH $H_{El}(x,y)$ as,

$$H_{El}(x, y) = H_l(x, y)\cdot C_l(x, y) + \alpha_l H_{l-1}(x, y) \quad (0.5 < \alpha_l < 1,\ 1 \le l \le K) \tag{6}$$

where $C_l(x,y)$ is used to encode the CGH $H_l(x,y)$, shown as Eq. (2). Because logic map sequences $X_l=\{a_{l0}, a_{l1}, a_{l2}, \ldots, a_{li}, \ldots, a_{lh}\}$ and $Y_l=\{b_{l0}, b_{l1}, b_{l2}, \ldots, b_{li}, \ldots, b_{lh}\}$ encoding the $C_l(x,y)$ could be