Available online at www.sciencedirect.com
ScienceDirect
Optik 121 (2010) 918–925
Optik Optics
www.elsevier.de/ijleo

Optical image encryption using improper Hartley transforms and chaos

Narendra Singh, Aloka Sinha*

Department of Physics, Indian Institute of Technology Delhi, Hauz Khas, New Delhi 110016, India

Received 22 June 2008; accepted 28 September 2008

Abstract

We propose a new method for image encryption using improper Hartley transform and chaos theory. Improper Hartley transform is a Hartley transform in which the phase between the two Fourier transforms is a fractional multiple of $\pi/2$. This fractional order is called fractional parameter and serves as a key in the image encryption and decryption process. Four types of chaos functions have been used. These functions are the logistic map, the tent map, the Kaplan–Yorke map and the Ikeda map. Random intensity masks have been generated using these chaotic functions and are called chaotic random intensity masks. The image is encrypted by using improper Hartley transform and two chaotic random intensity masks. The mean square error has been calculated. The robustness of the proposed technique in terms of blind decryption has been tested. The computer simulations are presented to verify the validity of the proposed technique.

Keywords: Image encryption/decryption; Improper Hartley transforms; Logistic map; Tent map; Kaplan–Yorke map

1. Introduction

In recent year, optical image encryption techniques have become very important in optical information processing. It has some attractive features such as fast computing and parallelism of optics which makes it very useful in the information security systems. A number of optical image encryption methods have been proposed. Optical image encryption using Fourier transform (FT) [1], fractional Fourier transform (FRT) [2–7], extended FRT [8,9], gyrator transform (GT) [10] and Fresnel transform (FrT) [11] have been proposed. Optical image encryption method based on moiré grating [12], water-making [13], polarized light [14], pixel scrambling [15] and lensless optical security system [16] have also been proposed. In all the above methods, the coherent illumination has been used in optical systems. Optical systems using incoherent light have advantages over the optical systems using coherent light. The requirements on the spatial-light modulator are relaxed because it does not need to record the phase. The incoherent optical systems are more practical than the coherent systems because the incoherent systems are free from coherent noises. The information recording using the incoherent optical system is easy in comparison to the coherent optical systems. Several researchers have proposed some incoherent optical systems for signal processing. An incoherent-only optical and electronic digital joint-transform correlator is proposed [17]. The FRT has been defined for working with incoherent light [18]. A method for securing and encrypting information optically by use of totally incoherent illumination has been proposed [19]. Hartley transform (HT) has been

*Corresponding author. Tel.: +91 11 2659 6003.
E-mail address: aloka@physics.iitd.ernet.in (A. Sinha).

0030-4026/$ - see front matter
doi:10.1016/j.ijleo.2008.09.049

used for optical image encryption method [20]. HT can be calculated by two FTs. There are two main properties of the HT. First, it is a real transform. Second, HT and its inverse transforms are identical [21]. Possibilities of the different types of the errors in two-dimensional optical HT have been evaluated [22]. The problem of bare decryption [23] in HT has been resolved by introducing the random intensity mask (RIM) at the input plane [24]. Recently, chaotic based encryption method using optical communication [25], Ikeda-based non linear delay dynamics [26] and optical ring resonators [27] have been proposed. Chaos functions are very sensitive to their initial conditions [28–30]. In optical image encryption techniques using RIM, the image is encrypted using RIMs and the whole random intensity mask has to be sent to the receiver side to decrypt the original image. Thus, the security of the data in these methods becomes less. In this paper, we propose a new technique of optical image encryption using improper HT and chaos. Improper HT is a HT in which the phase between two FTs is a fractional order multiple of $\pi/2$. This fractional order is called fractional parameter and serves as a key in the image encryption and decryption process. In the proposed technique, the image is encrypted using improper HT and the double RIM generated by the chaotic functions. These RIMs are called chaotic random intensity masks (CRIMs). In this method, the input image is multiplied by the first CRIM at the input plane and then improper HT is performed over it. Output image obtained is then multiplied by the second CRIM. After this process the encrypted image is obtained at the image plane. Four types of chaotic functions have been used to generate the CRIM. These functions are the logistic map, the tent map, the Kaplan–Yorke map and the Ikeda map. The mean square error (MSE) between the encrypted image and the input image and the decrypted image and the input image for correct and incorrect decryption process has been calculated. Robustness of the initial element called the seed value of the CRIM and the fractional parameter in terms of blind decryption has been tested.

2. The improper Hartley transform

The two-dimensional (2-D) HT [20,21] of a real function $f(x,y)$ is defined as

$$H(u,v)=\int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty} f(x,y)\,\mathrm{cas}[2\pi(ux+vy)]\,\mathrm{d}x\,\mathrm{d}y \tag{1}$$

and its inverse transform is defined as

$$f(x,y)=\int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty} H(u,v)\,\mathrm{cas}[2\pi(ux+vy)]\,\mathrm{d}x\,\mathrm{d}y, \tag{2}$$

where cas = cos + sin. According to the definition of the HTs, it is deduced as [20]

$$H(u,v)=\int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty} f(x,y)\,\mathrm{cas}[2\pi(ux+vy)]\,\mathrm{d}x\,\mathrm{d}y \tag{3}$$

$$=\frac{\exp(\mathrm{i}\pi/4)}{\sqrt{2}}[F(u,v)+\exp(-\mathrm{i}\pi/2)F(-u,-v)]. \tag{4}$$

In the HT operation, the term $\exp(\mathrm{i}\pi/4)/\sqrt{2}$ can be ignored [21] because the output obtained is an intensity information i.e. the square of the amplitude in which this term will be canceled. It is noted that the HT can be calculated by two FTs and the phase between the two FTs is $\exp(-\mathrm{i}\pi/2)$. At this value of phase, the relative strength of the cosine and sine transform will be equal to each other and the information about the odd and even part of the input object will be equally represented [22]. In the proposed technique, a fractional parameter 'p' is introduced in the phase between the two FTs. The HT with fractional parameter 'p' is represented as

$$H^p(u,v)=\frac{\exp(\mathrm{i}\pi/4)}{\sqrt{2}}[F(u,v)+\exp(-\mathrm{i}p\pi/2)F(-u,-v)], \tag{5}$$

where 'p' is called fractional parameter and bounded between 0 and 1. This HT is called improper HT. For $p=1$, the improper HT is equivalent to the HT. For value of 'p' other than 1, the output remains real but the relative strength of the cosine and sine transform will no longer be equal and thus information about the odd and the even part of the input object will be represented improperly. So this HT with fractional parameter 'p' is called improper HT.

3. Chaotic functions

Chaotic functions are defined as functions that generate random values or iterations. Chaotic functions have several interesting properties. These functions are very sensitive to the initial conditions. These functions generate random iterative values. Convergence of the iterative values after any value of iterations can never be seen. Four chaos functions have been used for our study. The first chaotic function is the logistic map [28–30]. It is defined as

$$f(x)=p\cdot x\cdot(1-x). \tag{6}$$

This function is bounded for $0<p<4$. The iterative form of this function is written as

$$x_{n+1}=p\cdot x_n\cdot(1-x_n) \tag{7}$$

with 'x_0' as the initial value. This is also known as the seed value for the chaotic function. The second chaos