Optics and Lasers in Engineering 51 (2013) 967–972

Contents lists available at SciVerse ScienceDirect

Optics and Lasers in Engineering

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

Optical color image hiding scheme based on chaotic mapping and Hartley transform

Zhengjun Liu [a,b,c,e,*], Yu Zhang [a,**], Wei Liu [d], Fanyi Meng [c], Qun Wu [c], Shutian Liu [d]

[a] Department of Automatic Measurement and Control, Harbin Institute of Technology, Harbin 150001, China
[b] State Key Laboratory of Transient Optics and Photonics, Chinese Academy of Sciences, Xi'an 710119, China
[c] Department of Electronic Science and Technology, Harbin Institute of Technology, Harbin 150001, China
[d] Department of Physics, Harbin Institute of Technology, Harbin 150001, China
[e] State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China

ARTICLE INFO

Article history:
Received 17 December 2012
Received in revised form
2 February 2013
Accepted 20 February 2013
Available online 19 March 2013

Keywords:
Optical encryption
Cryptography
Chaotic mapping

ABSTRACT

We present a color image encryption algorithm by using chaotic mapping and Hartley transform. The three components of color image are scrambled by Baker mapping. The coordinates composed of the scrambled monochrome components are converted from Cartesian coordinates to spherical coordinates. The data of azimuth angle is normalized and regarded as the key. The data of radii and zenith angle are encoded under the help of optical Hartley transform with scrambled key. An electro-optical encryption structure is designed. The final encrypted image is constituted by two selected color components of output in real number domain.

1. Introduction

Information security of color image has been considered based on the encryption algorithms of gray-level image, such as random phase encoding [1], digital holography [2] and coherent diffractive imaging [3]. The encryption schemes of one or two color images [4–7] have been designed by using double random phase encoding [8,9]. Three kinds of optical color encryption approaches have been reported by using interference technique with Arnold transform [10–12]. A color image encryption method has been represented by use of the rotation of color vectors in Hartley domains [13]. Combining the Arnold transform and color-blend operations, a color image method has been proposed [14]. A dynamical color encryption algorithm has been represented by hiding the information from the three components [15]. The multi-color visual cryptography has been introduced for information security [16]. The Hartley transform has been applied in color image encryption with random phase encoding or other transforms [17–20]. In most of these color encryption schemes mentioned above, the three components of color image are separated to be hidden as three gray-level images. The final encrypted image is encoded into a color image with RGB components in complex number domain or real number domain. In addition, triple- or multiple-image encryption methods [21–24] can serve as a potential method encoding color image, in which the encrypted image; however, is gray-level.

In this paper, an optical color image algorithm is developed by employing chaotic mapping and Hartley transform. The three components of color secret image are randomized by Baker mapping, which is a scrambling operation [25–29], and are transformed into the spherical coordinates. The data of normalized azimuth angle, which is random, is extracted and regarded as key. Two functions are defined by radii and zenith angle. Subsequently the two functions are scrambled by chaotic mapping and Hartley transform. The two functions are encoded into two components of the final encrypted color image, where another component has no information and is replaced with 0, in real number domain. An optical system is given to implement the encryption algorithm. Some numerical results have been shown for demonstrating the performance of the proposed encryption scheme.

2. Color encryption algorithm

A color image $I_0(x,y)$ is decomposed as a vector as follows:

$$I_0(x,y) = [R_0(x,y), G_0(x,y), B_0(x,y)], \quad (1)$$

where R_0, G_0 and B_0 are RGB components. Baker mapping [29] is

* Corresponding author at: Department of Automatic Measurement and Control, Harbin Institute of Technology, Harbin 150001, China. Tel.: +86 451 86413151; fax: +86 451 86415146.
** Corresponding author.
E-mail addresses: zjliu@hit.edu.cn, zjliuv@gmail.com (Z. Liu), hitzhangyu@gmail.com (Y. Zhang).

0143-8166/$ - see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.optlaseng.2013.02.015

introduced for pixel scrambled and is defined as:

$$y' = \frac{N}{n_j}(y - N_j) + \mathrm{mod}\left(x, \frac{N}{n_j}\right), x' = \frac{n_j}{N}\left[x - \mathrm{mod}\left(x, \frac{N}{n_j}\right)\right] + N_j,$$
$$0 \le x, y < N, \sum_{\forall j} n_j = N, N_j = n_1 + \cdots + n_j, N_0 = 0, \tag{2}$$

where (x,y) and (x',y') are pixel position in discrete case before and after the mapping, respectively. The parameter N represents the size of the squared image. The sequence n_j is the main parameters of Baker mapping. Here a limiting condition is that the value of N/n_j is integer. A pixel scrambling relation is expressed as

$$R'_0(x,y) = \mathscr{B}_{j_1 n_j}[R_0(x,y) - m],$$
$$G'_0(x,y) = \mathscr{B}_{j_2 n_j}[G_0(x,y) - m],$$
$$B'_0(x,y) = \mathscr{B}_{j_3 n_j}[B_0(x,y) - m], \tag{3}$$

where the symbol '$\mathscr{B}$' is Baler mapping operator, in which different parameters n_j are used for randomizing the three components and $\{j_1, j_2, j_3\}$ are the total iterative number of the mapping. The parameter m is an expected mean value and is fixed at 128 for 8-bit image in this paper. The scrambled components (R'_0, G'_0, B'_0) are considered for expressing the points in Cartesian coordinates and are converted into spherical coordinates as follows:

$$r(x,y) = \sqrt{R'^2{}_0(x,y) + G'^2{}_0(x,y) + B'^2{}_0(x,y)},$$
$$\theta(x,y) = \mathrm{atan2}(G'_0(x,y), R'_0(x,y)),$$
$$\phi(x,y) = \mathrm{acos}(B'_0(x,y)/r(x,y)), \tag{4}$$

where the function 'atan2' is to compute four quadrant inverse tangent. The azimuth angle θ is normalized by:

$$K(x,y) = \frac{\theta(x,y)}{2\pi}, \tag{5}$$

where the function $K(x,y)$ serves as the main key of this encryption algorithm. Two functions i_1 and i_2 are given as:

$$i_1(x,y) = r(x,y)\cos[\phi(x,y)], i_2(x,y) = r(x,y)\sin[\phi(x,y)] \tag{6}$$

A random data $K_1^{(p_1)}(x,y)$ is generated by logistic mapping [30,31] and Baker mapping as

$$T(x,y) = \alpha \cdot K_1^{(p-1)}(x,y)[1 - K_1^{(p-1)}(x,y)],$$
$$K_1^{(p)}(x,y) = B_{k,n_j}[T(x,y)], \tag{7}$$

where $p = 1,\ldots,p_1$. $K_1^{(0)}(x,y) = K(x,y)$. The coefficient α is the parameter of logistic map and is limited in the range [3.57, 3.82]. The i_1 and i_2 are encoded by an affine transform as:

$$\begin{bmatrix} i'_1 \\ i'_2 \end{bmatrix} = \begin{bmatrix} 1 + c_1\cos\beta & 0 \\ 0 & \frac{1}{1 + c_2\sin\beta} \end{bmatrix} \begin{bmatrix} \cos\beta & -\sin\beta \\ \sin\beta & \cos\beta \end{bmatrix} \begin{bmatrix} i_1(1 + c_1\cos\beta) \\ \frac{i_2}{1 + c_2\sin\beta} \end{bmatrix}, \tag{8}$$

where $\beta = 2\pi K_1^{(p_1)}(x,y)$. The functions $i'_1(x,y)$ and $i'_2(x,y)$ are output. The parameters c_1 and c_2 are constant and are located in the interval (0, 1).

Hartley transform is introduced for changing the data of the functions $i'_1(x,y)$ and $i'_2(x,y)$. The transform [32,33] is expressed as:

$$\begin{aligned} H(u,v) &= \mathscr{H}[h(x,y)](u,v) \\ &= \iint h(x,y)\mathrm{cas}(2\pi xu + 2\pi yv)dxdy \\ &= \mathrm{Re}\{\mathcal{F}[h(x,y)](u,v)\} + \mathrm{Im}\{\mathcal{F}[h(x,y)](u,v)\}, \end{aligned} \tag{9}$$

where h and H are the input and output of Hartley transform. The operators '$\mathscr{H}$' and '$\mathcal{F}$' are Hartley transform and Fourier transform, respectively. The function 'cas(…)' is equal to 'cos(…)+sin(…)'. Optical Hartley transform is in real number domain. By using Hartley transform, $i'_1(x,y)$ and $i'_2(x,y)$ are altered as follows:

$$I_1(u,v) = \mathscr{H}[i'_1(x,y)](u,v), I_2(u,v) = \mathscr{H}[i'_2(x,y)](u,v). \tag{10}$$

To enhance the security of encryption algorithm, Eqs. (7), (8) and (10) will be performed three or more times. During the iteration, some parameters in chaotic mapping can be taken at different values. The two encoded functions will be regarded as

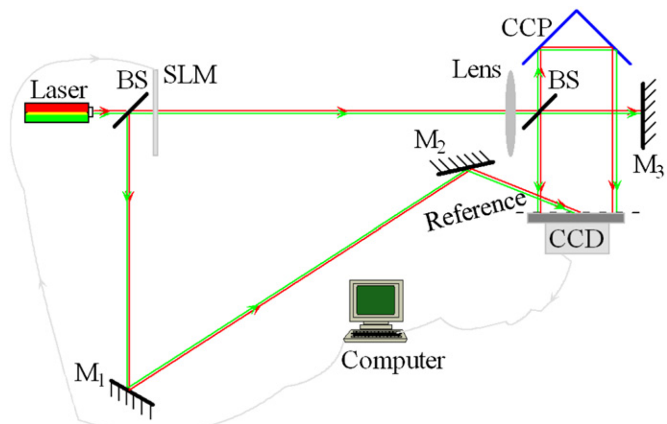

Fig. 1. Optical color image encryption system.

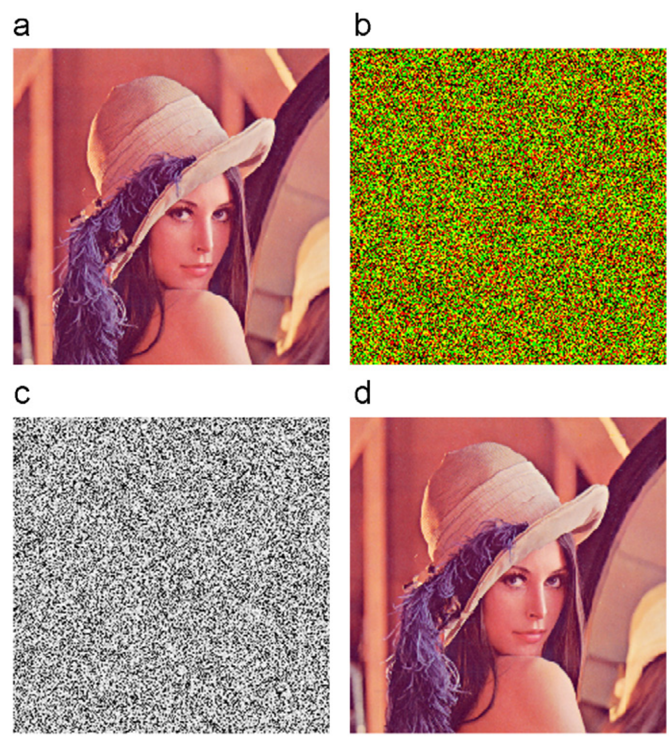

Fig. 2. Encrypted results: (a) original image, (b) encrypted image, (c) the distribution of key K and (d) decrypted image.

Table 1
The parameters of Baker mapping.

	n_j												j_k $k=1,2,3$
$\mathscr{B}_{j_1,n_j}$	16	8	32	64	32	16	32	8	16	32	/	/	40
$\mathscr{B}_{j_2,n_j}$	8	8	16	16	32	32	64	8	16	32	16	8	40
$\mathscr{B}_{j_3,n_j}$	16	32	16	8	16	64	32	8	32	8	8	16	40